

GOVERNMENT DEMANDS FOR ELECTRONIC EVIDENCE: IS RESISTANCE FUTILE?

Kurt Stitche[†]
Levenfeld Pearlstein, LLC
Chicago, Illinois
Copyright © 2008 Kurt Stitche

Government demands for the production of electronic evidence come in two basic forms: grand jury subpoenas *duces tecum* and search warrants. While the power of a grand jury to compel the production of electronically-stored information (“ESI”) is extremely broad, a client may still negotiate the scope of, or object to, a grand jury subpoena **before** producing anything, thereby protecting privileged and confidential information. In the case of a search warrant, however, the client has no such *ex ante* ability to negotiate or to object. Thus, in the age of ESI, the execution of a search warrant may lead to the seizure of extraordinary volumes of irrelevant, privileged, and/or protected data, including those belonging to third parties. Because the courts have shown little inclination to adapt their Fourth Amendment “search and seizure” jurisprudence to the realities of our digital culture, clients may have to engage in some “self-help” to ensure that their sensitive information, and that of **their** clients, remains protected. This article discusses the threats to our privacy in the age of ESI search and seizure and suggests some possible steps for preventing disclosure of protected electronic information.

I. GRAND JURY SUBPOENAS *DUCES TECUM*

A. Authority and Oversight

Rule 17(c) of the Federal Rules of Criminal Procedure authorizes a grand jury to compel the production of “books, papers, documents, data, or other objects the subpoena designates.”¹ Indeed, the grand jury’s power to subpoena non-testimonial information is quite broad, and the Government’s demands, often quite sweeping.² Moreover, the Government’s documentary subpoena power is not subject to the strictures of the Fourth Amendment, which governs only “searches and seizures” of information.³ In the context of a subpoena *duces tecum*, by contrast, the recipient of the subpoena still controls the materials demanded and can object to the scope of the subpoena before any production (“seizure”) occurs.⁴ Because the “intrusion” of a subpoena *duces tecum* is much less significant than that of a search warrant, the courts generally apply a lower threshold of “reasonableness” than in the Fourth Amendment context.⁵

[†] Kurt Stitche, a former federal prosecutor, is a Partner at Levenfeld Pearlstein, LLC, in Chicago, Illinois, where he heads up the firm’s White Collar Criminal Defense and Corporate Internal Investigations practice. Mr. Stitche may be reached at (312) 476-7597 or at kstitche@lplegal.com. The author gratefully acknowledges the assistance of Scott A. Meyers, James G. Martignon, Deepa Rajkarne, Melissa Mistretta, Daniel Mullenix, and Whitney Merritt in the review and editing of this article. The viewpoints expressed in the article are, however, solely those of the author.

The Government's subpoena power is not, of course, wholly beyond the control of the courts, as "[g]rand juries are subject to judicial control and subpoenas to motions to quash."⁶ As a practical matter, however, the only limitation on the Government's power in this regard is the requirement that a subpoena *duces tecum* be "reasonable."⁷ "Reasonableness," in turn, generally hinges on the relevance of the demands to the investigation, the particularity of the demands, and the burden placed on the subpoenaed party, in terms of scope and time frame.⁸ In any challenge to a subpoena *duces tecum*, the subpoenaed party bears the burden of proving "unreasonableness," and the courts are highly deferential to the grand jury in this regard.⁹

B. Negotiations over Scope and Privilege

As both a legal and a practical matter, a subpoena recipient is well-advised to negotiate limitations before asking the court to quash or modify a subpoena *duces tecum*. First, some courts have considered the recipient's efforts to confer with the Government over the subpoena's scope when assessing the recipient's "burdensomeness" objection.¹⁰

Second, the Government is usually amenable to reasonable restrictions on the scope of a subpoena *duces tecum*, because (a) the Government knows that it tends to draft such subpoenas in an extremely broad manner, and (b) once the subpoena recipient makes clear its intent to cooperate fully, prosecutors are generally open to discussion about how they can obtain the greatest amount of relevant information in the shortest period of time.

As such, counsel for a recipient of a subpoena seeking ESI should, after careful consultation with the client, approach the Government to negotiate reasonable restrictions on the scope of the subpoena. Such restrictions typically include (a) a narrower time frame; (b) a limitation on the number of "custodians" whose files must be searched; and/or (c) specific search terms ("keywords") that will guide the client's efforts to collect responsive ESI.¹¹

In addition, given the prominence of privilege considerations in the production of mass quantities of ESI, counsel should seek agreement with the Government regarding the "inadvertent production" of privileged materials. Although such inadvertent production may or may not constitute a waiver of privilege (and, thus, the Government may or may not have to return such privileged materials), the Government does have some incentive to reach agreement, because subpoena recipients are typically able to produce documents more quickly when they do not have to engage in a painstaking, document-by-document privilege review.¹²

Even if the Government refuses to accommodate the client on this point, all hope is not lost. First, the law of inadvertent waiver is in flux, with the courts trending toward greater protection for privileged materials disclosed in this manner.¹³ Thus, depending on the jurisdiction, and on the facts underlying the inadvertent production, the client may be able to recover its privileged documents and avoid any waiver of protections.

Second, Congress is currently debating proposed Federal Rule of Evidence 502, which would dramatically strengthen a subpoenaed party's claims that its inadvertent production of privileged information does not constitute a waiver of any privilege.¹⁴ The addition of Rule 502

would go a long way toward providing some degree of comfort to subpoenaed parties and minimizing protracted battles over alleged waivers of privilege.¹⁵

C. Motions to Quash

If the Government is not amenable to reasonable restrictions in the foregoing areas, the client may wish to seek court intervention through a Motion to Quash. As noted earlier, the outright quashing of a subpoena *duces tecum* is – in light of subpoena standards and the court’s deference to the grand jury’s broad authority – highly unlikely.¹⁶ Nevertheless, courts unequivocally have the power to **modify** subpoenas where full compliance would be unreasonable or oppressive.¹⁷ As such, to the extent that Government intransigence may impose undue burdens on a party from whom the Government has demanded wide-ranging electronic document production, the court may intervene to impose reasonable limitations on scope.¹⁸

If the subpoena recipient is an individual, she may also move to quash the subpoena if compliance would violate her Fifth Amendment privilege against self-incrimination under the “act of production” doctrine. Under this doctrine, the court may quash a subpoena where the compelled production of otherwise unprivileged information could implicitly communicate incriminating facts, such as the existence, custody and control, or authenticity, of the questioned information.¹⁹

Finally, it should be noted that the recipient of a grand jury subpoena *duces tecum* is not the only party who can contest its scope, as the courts have held that third parties whose legitimate interests – such as privacy or privilege – might be infringed by compliance with the subpoena also have standing to challenge it.²⁰ The importance of this right cannot be underestimated, because the inevitable delay between receipt of a subpoena and compliance therewith affords the recipient the opportunity to **notify** affected third parties about the subpoena’s existence and scope, thus allowing those third parties to intervene to protect their interests. As we will see later in this article, search warrants do not provide interested third parties with such an opportunity.

D. Summary

As the foregoing suggests, a client faced with a subpoena *duces tecum* maintains at least some amount of **control** over the process. First, there is no government intrusion onto the client’s property, and the client can choose to cooperate or to challenge the subpoena prior to any production. Which direction the client takes will often depend on its ability to **negotiate** the terms of the subpoena before responding thereto. Even failing negotiations, however, the client can turn to the **courts** for an *ex ante* ruling on the scope of any necessary production. Likewise, the client can notify affected third parties, who may also seek the court’s assistance.

Second, when producing responsive documents, the client can **segregate** – and avoid producing – irrelevant information that is “intermingled” with responsive data in its computer system. Such segregation and exclusion from production would, of course, include **privileged** materials.

Third, though not addressed in detail above, the client can **track** its production of ESI by reviewing documents prior to production, maintaining an exact electronic copy of all information produced, and Bates-numbering individual electronic documents for future use.²¹

As the following section shows, this degree of control simply does not exist in the context of search warrants for electronic evidence.

II. SEARCH WARRANTS

A. Authority and Oversight

Rule 41 of the Federal Rules of Criminal Procedure governs the issuance of search warrants. For the purposes of this article, the critical provisions of Rule 41 are those that (a) expressly provide for the issuance of warrants seeking ESI;²² (b) vest a United States Magistrate Judge with authority to issue warrants;²³ (c) include “evidence of a crime” among the “property subject to search or seizure;”²⁴ (d) require a finding of “probable cause” before a warrant can issue;²⁵ and (e) command identification, in the warrant, of any property to be searched and/or seized.²⁶

As Rule 41 itself provides, a federal Magistrate Judge oversees all federal search warrants on an *ex ante* basis. That is, the Magistrate must find probable cause to justify the search and seizure, and he must pass on the scope of the search and seizure with reference to the property specifically identified in the warrant, **before** the warrant will issue.²⁷

In light of Rule 41’s requirements, the U.S. Department of Justice has drafted detailed guidelines for federal agents who are applying for a warrant to search for ESI.²⁸ Setting aside the threshold issue of establishing “probable cause” to believe that relevant evidence will be found in the place(s) to be searched, the DOJ advises agents to specify the **scope** of the search in its warrant submissions, which should include reference to (a) the crime(s) being investigated; (b) the target(s) of the investigation; (c) the relevant time period; (d) the particular ESI sources to be searched; (e) the role of those data sources in the alleged crimes; and (f) a **strategy** for conducting the search.²⁹ It is the last of these items, search strategy, that raises the most vexing questions in the logistics of searches for electronic evidence, an issue that we will address in some detail below.

B. Constitutional Limitations

In addition to the requirements set forth in Rule 41, the Fourth Amendment to the United States Constitution and the extensive case law interpreting it represent another source of limitation on the power of the Government to search for and seize ESI. The Fourth Amendment provides that

[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

describing the place to be searched, and the persons or things to be seized.³⁰

The Fourth Amendment is much broader than Rule 41, in that the United States Supreme Court has interpreted the Amendment to protect essentially anything in which an individual has a subjective expectation of privacy, as long as society accepts that expectation as objectively “reasonable.”³¹ The Court’s Fourth Amendment jurisprudence also extends well beyond searches and seizures conducted pursuant to valid warrants, a topic outside the purview of Rule 41 (and of this article).

1. Probable Cause

Like Rule 41, however, the Fourth Amendment explicitly concerns itself with “probable cause” in the context of search warrants. Stated simply, “probable cause” exists where “the facts and circumstances within the [federal agent’s] knowledge, and of which he has reasonably trustworthy information, are sufficient in themselves to persuade a person of reasonable caution to believe the search is justified.”³² Probable cause does not require certainty, merely a reasonable belief that the material to be seized will be found during a search of the designated property.³³ The courts assess the “reasonableness” of such a belief under a “totality-of-the-circumstances” standard, based on facts known at the time the agent applies for the warrant.³⁴ In short, the “probable cause” threshold is less than onerous.

2. Particularity

The Fourth Amendment also concerns itself with Rule 41’s “particularity” requirement, which incorporates identification not only of the **place** to be searched, but the specific **items** to be searched for and seized once there.³⁵ The purpose of this prerequisite is to remove from the searching agents all discretion as to what can be searched and seized,³⁶ thereby eliminating the abuse of the “general warrant” and the “writs of assistance” prevalent at the time of our nation’s independence.³⁷

In the context of searches for contraband, fruits of crime, or “mere evidence” **within** computers, “particularity” requires specification of the ESI to be searched and seized, not merely of the physical structure that houses those data.³⁸ If the search warrant is inadequate on this point, the courts may find the warrant invalid and the search, unlawful.³⁹ Contrarily, as long as the warrant specifies a time frame, the alleged criminal activity, and the type of evidence the agents expect to find, the courts will almost certainly uphold the warrant against a “particularity” challenge.⁴⁰

C. Practical Problems in Computer Searches and Seizures

1. The Volume of Electronically-Stored Information

Setting aside such metaphysical issues as whether electronic data stored on a computer even exists in “physical” form or whether such storage mechanisms can be analogized to “closed containers” for Fourth Amendment purposes, there exist several practical, logistical problems in

the search and seizure of ESI. The first of these is the sheer volume and complexity of information that may be stored on a computer hard drive. As one commentator describes it:

No longer merely word processors or data aggregation tools, computers now function as diaries, photo albums, stereos, telephones, desktops, file cabinets, waste paper baskets, and televisions. Computers have storage capacities greater than ever before; today, most basic personal computers come with at least eighty gigabytes of storage, the equivalent of forty million pages of text or eighty thousand books. In addition to storing the documents and files users consciously save, computers also typically record “metadata” – information about the creation and modification of documents – as well as data deleted by the user, which investigators may be able to recover fully or partially. Computers also store information about the websites a user has visited on the Internet. With sixty-six percent of all homes in the United States containing computers, and their massive ability to retain information for and about their users, courts have become increasingly concerned about balancing privacy interests against the government’s need to search electronic storage devices.⁴¹

Thus, federal agents executing a search warrant for computer information face the prospect of locating the proverbial “needle in the haystack,” as they may have to sift through tens (or hundreds or thousands) of millions of pages of documents to find those identified in the warrant.

The possibility of such searches has rendered the old “search and seizure” paradigm moot. In the olden days, agents simply searched the area specified in the warrant (*e.g.*, a house, a union hall, a warehouse) until they came upon, and seized, the type of documents specified in the warrant. In the computer age, however, agents must **search** the specified area in order to **seize** the computers contained therein, then **search** those computers in order to **seize** the **information** identified with particularity in the warrant.⁴² This new paradigm renders quaint notions of “open containers” and “closed containers” hopelessly outdated.

2. The Structure of Electronically-Stored Information

a. Relational Databases and “Intermingling”

Even more problematic than the volume of ESI in a typical computer is the structure and location of those data. Again, without delving into the metaphysical, it is axiomatic that modern computer databases are “relational,” such that no matter how well-specified the sought-after data may be, they will be found among gigabytes of information that are unrelated and outside the scope of the warrant. As even the U.S. Department of Justice recognizes:

Searches for computer files tend to be more complicated. Because computer files consist of electrical impulses that can be stored on the head of a pin and moved around the world in an instant, agents may not know where computer files are stored, or in what form.

Files may be stored on a floppy diskette, on a hidden directory in a suspect's laptop, or on a remote server located thousands of miles away. The files may be encrypted, misleadingly titled, stored in unusual file formats, or **commingled with millions of unrelated, innocuous, and even statutorily protected files**. As a result of these uncertainties, agents cannot simply establish probable cause, describe the files they need, and then “go” and “retrieve” the data.⁴³

The complexity of searches for ESI can hardly be overstated. Digital data are simply collections of “ones” and “zeros” organized into groups, typically known as clusters (the smallest grouping) and sectors (a collection of clusters).⁴⁴ A single document may span multiple clusters, which may, in turn, be physically stored in any open space on a computer hard drive. Thus, in order to retrieve even a single document, the computer must track the various clusters storing the data for that document and interpret which part of the document is stored in which cluster. Even the deletion of the document does not change this analysis, because when a computer user “deletes” information, the computer merely marks the disk space that the document occupies as “available” for new data. Until that space is **actually** occupied (overwritten with new data), however, the document still exists and can be tracked and recovered.⁴⁵

Practically speaking, then, **all** electronically-stored information is “intermingled,” and specific data cannot be “seized” without some type of “search” to locate and retrieve it.⁴⁶ Add to this equation the fact that much ESI is stored not on the hard drive of an individual's personal computer, but on servers that may process information for untold numbers of users within a network, whether formal (*e.g.*, a business) or informal (*e.g.*, a chat room),⁴⁷ and it quickly becomes apparent that the scope of any computer search will almost ineluctably be vastly overbroad. Unfortunately, the intermingling inherent in relational databases has flummoxed the courts, which have pointed to intermingling as justification for broad seizures of data.⁴⁸

b. Search Methodology and Location

Critics of sweeping seizures of ESI (including those whose ESI has been searched) have argued that even if the Government cannot identify, *ex ante*, exactly where it will find the data specified in the warrant, it can, at the very least, provide the Magistrate with a search **methodology** designed to locate such data. The courts have almost uniformly rejected this suggestion.⁴⁹ Not only do many courts believe that Magistrates are not well-equipped to appreciate the complexities of computer searches,⁵⁰ but the courts generally manifest skepticism about methodologies – such as “keyword” searching – that would improve a criminal's odds of hiding ESI described in the search warrant.⁵¹

Because all ESI is stored in a “relational” manner, and because *ex ante* methodologies to limit the scope of a search appear impractical, the odds of the Government conducting a computer search at the client's location are close to nil. Indeed, as much of the foregoing case law has made clear, the courts routinely uphold the wholesale seizure of computer hardware, software, peripherals, and data for off-site review.⁵² Likewise, DOJ prefers off-site searches, due to logistical constraints, minimized intrusion, and considerations of data handling.⁵³

Because the courts do not hesitate to uphold the wholesale seizure (or, at a minimum, wholesale copying) of electronically-stored information, and because the Government manifestly prefers such seizures, it is essentially unavoidable that the execution of a search warrant at your client's home or office will sweep up materials well beyond the scope of the warrant, including (a) materials protected from disclosure by one or more privileges, (b) materials that implicate your client's right to privacy (or that of third parties); (c) materials as to which no probable cause to search or seize exists; and (d) materials relating to third parties as to whom no probable cause to search or seize exists.

3. Scope of the Post-Seizure Search

And the client's problems do not end when the seizure ends. Once the Government has possession of the client's ESI, the Government will search it for information responsive to the warrant, a process over which your client will have no effective *ex ante* control. How will the Government search the data? Reflect on what we have learned to date: the volume of data is extraordinary; relevant materials are "intermingled" with privileged and irrelevant data; forensic analysis is "more of an art than a science;"⁵⁴ and real criminals are inclined to conceal incriminating data.⁵⁵ The likely result? Very broad, detailed searches for the information identified in the warrant, the kind of broad, detailed searches that are likely to uncover every type of sensitive information described above.

And what if, during such a search, the Government comes across ESI outside the scope of the warrant, that is to say, information for which no probable cause existed when the warrant was obtained and which is not described with particularity in the warrant? Under the "plain view" doctrine, odds are good that the Government will be able to use it against your client. Although a full discussion of "plain view" jurisprudence is beyond the scope of this article, the doctrine essentially allows a government agent to seize, without a warrant, any property discovered during an otherwise lawful search, if the incriminating nature of the property is immediately apparent.⁵⁶

In the context of computer searches, the courts have – with only minor qualification – upheld the warrantless "plain view" seizure of facially incrimination information during a lawful search of ESI.⁵⁷ And even where the courts disapproved of a plain view seizure, the Government could have remedied its Fourth Amendment violations simply by seeking proper warrants to pursue the searches at issue.⁵⁸ In short, there appear to be precious few limitations on the Government's power to "seize and search" electronically-stored information, and certainly none that allows the client to control its own destiny by withholding irrelevant or protected materials.

D. Challenges to Electronic Search and Seizure

1. Pre-Indictment Challenges

a. Rule 41(g) Jurisprudence

Despite the foregoing, the Federal Rules of Criminal Procedure do provide a mechanism for contesting the scope of a Government seizure of ESI. Specifically, Rule 41(g) allows “[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property” to file a “Motion to Return Property” in the court whence the warrant issued.⁵⁹ Where the allegation is one of an unlawful search or seizure, the movant – whether the owner of the property searched and seized or the ultimate victim of the improper search and seizure – must establish a Fourth Amendment violation; if successful, the court may order the seized property returned.⁶⁰ The court may also **deny** return, however, if the Government can establish a claim to the materials that is consistent with Fourth Amendment jurisprudence, such as through the “good faith” exception to the exclusionary rule,⁶¹ or through case law that legitimizes certain uses of illegally seized evidence.⁶² At base, Rule 41 does not “trump” either Fourth Amendment jurisprudence or federal statutes when it comes to the use of illegally-obtained evidence.⁶³

Where the seizure was lawful, but the movant has nonetheless been “aggrieved” by the deprivation of property, the standard for obtaining a return of property is even higher.⁶⁴ First, the movant must convince the court to exercise its equitable (or “anomalous”) jurisdiction over the dispute. In order to do so, the movant must demonstrate irreparable harm and an inadequate remedy at law.⁶⁵ Second, even if the movant is able to secure jurisdiction, he must, in order to prevail on the merits, show that the Government’s lawful possession of the ESI is “unreasonable.”⁶⁶ In this regard, the courts assess whether the Government has a continuing need for the property for purposes of investigation or prosecution. If so, the retention is generally deemed to be reasonable. If not, the property should be returned to its rightful owner.⁶⁷

In the context of ESI seizures, and as the Government unabashedly concedes, Rule 41(g) motions rarely succeed.⁶⁸ First, the courts will typically decline to exercise jurisdiction over the dispute where the Government offers to provide the property owner with a copy of any seized ESI.⁶⁹ Second, even when the courts reach the merits of the dispute, return is rarely ordered, because the courts typically find that the Government’s need for the data outweighs the movant’s, as long as a criminal investigation or prosecution, or a civil forfeiture matter, is proceeding.⁷⁰

b. The Ninth Circuit’s “BALCO” Opinion

On December 27, 2006, the Ninth Circuit Court of Appeals handed down its opinion in *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915 (9th Cir. 2006), a case that illustrates most poetically all of the difficulties that the victims of an overly broad search and seizure may encounter when trying to protect their cherished right of privacy. As such, this opinion, which we will call “BALCO” for short, is worth exploring in some detail.

(1) Factual Background

During its investigation into the illegal distribution of steroids to Major League Baseball (“MLB”) players through the Bay Area Laboratory Cooperative (“BALCO”), the Government identified 10 MLB players whom, it had probable cause to believe, received steroids from BALCO. The Government then served a grand jury subpoena on MLB for all drug testing records of those 10 players (and, for unknown reasons, an additional player), but MLB responded that it had no such records.⁷¹

Having been rebuffed by MLB, the Government served grand jury subpoenas *duces tecum* on the two testing laboratories, Comprehensive Drug Testing, Inc. (“CDT”), and Quest Diagnostics, Inc. (“Quest”), that had processed drug testing samples for MLB. The subpoenas sought testing for “all MLB players,” a request to which CDT and Quest informally objected as overbroad. The Government then reissued the subpoenas to include only the 11 players named in the MLB subpoena.⁷²

When the MLB Players’ Association (“the Players’ Association”) told the Government that it intended to move to quash the reissued subpoenas, the Government obtained search warrants for CDT’s and Quest’s premises from Magistrate Judges sitting in the two companies’ respective judicial districts. These warrants identified their targets as the original 10 MLB players and authorized the Government to seize computers if an on-site search was “impractical.”⁷³

The day after the Players’ Association and CDT filed their motions to quash the reissued subpoenas, the FBI executed the search warrant at CDT’s facilities. CDT management called its outside counsel, who attempted to negotiate the scope of the computer searches with the Government. After FBI agents threatened to seize and remove all of CDT’s computers, CDT personnel reluctantly identified for the agents a specific computer directory that contained results for **all of CDT’s sports drug testing programs**. The FBI then copied the entire directory for later review at its offices.⁷⁴

Eighteen days later, the Players’ Association filed Rule 41(g) motions for the return of property, seeking the return of all information that did not relate to the 10 MLB players specified in the two search warrants. Unfortunately for the Players’ Association, the Government had already reviewed the contents of the directory it had copied and had used the information gleaned from that review to obtain two new search warrants for specimens and records relating to over 100 professional athletes whose information appeared in the seized CDT materials. Immediately after the execution of those warrants at CDT and at Quest, the Players’ Association filed additional Rule 41(g) motions seeking the return of all such records seized.⁷⁵

Finally, perhaps in an effort to cover all of its bases, the Government served new grand jury subpoenas on CDT and Quest, which demanded production of the same type of information that the Government had just seized that same day during the execution of the search warrants. The Players’ Association then moved to quash these subpoenas.⁷⁶

Upon hearing the various Rule 41(g) motions, federal district court judges in Nevada and the Central District of California ordered the Government to return to CDT and Quest all seized materials, except those relating to the 10 MLB players specified in the original warrants.⁷⁷

(2) Majority Opinion

The majority began its opinion by assessing whether the Players' Association had standing to contest the search of Quest's facilities, a question that it answered in the affirmative.⁷⁸ In doing so, the majority held that each of the MLB players whose drug test results were seized would have had standing to contest the seizure, even though they had no interest in the facilities searched and were not present for the search.⁷⁹

The majority then moved on to a consideration of the four factors governing the district courts' exercise of equitable jurisdiction, in order to assess whether such exercise was proper. Because the Government conceded one of the four factors, and the majority readily found in the Players' Association's favor on two more, it devoted most of its time to discussing whether the Government had, through the use of multiple subpoenas and search warrants, evinced a "callous disregard" for the constitutional rights of the players,⁸⁰ a query that the majority answered in the negative.⁸¹

To support its ultimate conclusion, the majority set forth two subsidiary conclusions. First, the majority held that the Government did not act wrongfully when it served multiple grand jury subpoenas and search warrants demanding the same information. According to the majority, because different standards govern the issuance of each demand and because recipients can challenge them in different ways, the two mechanisms are not mutually exclusive.⁸²

Second, the majority noted that the warrants specifically authorized the seizure of computers if on-site searching was impractical. In this case, the majority found, the Government had acted reasonably in seizing a mirror image (bitstream copy) of the relevant directory, even where files identified in the warrant were intermingled with information outside the scope of the warrant, because the warrant permitted such a broad seizure.⁸³ The majority also held that the Government had no obligation to conduct "keyword" searches or to rely on the "searched party" to retrieve responsive documents, because the Government would have had no assurance that it was collecting all necessary information.⁸⁴

Proceeding to the merits of CDT's Rule 41(g) motions, the majority weighed the Government's continuing need for the seized information against CDT's right to its property under a "reasonableness" standard.⁸⁵ In this case, the majority found, there was no reasonable basis for CDT's request, because the Government had already provided CDT with copies of all information seized, and the Government needed its copies for an expanded grand jury investigation into other possible MLB steroid users.⁸⁶ The majority cautioned, however, that the Government had not complied with *Tamura's* requirement of an off-site review by a neutral magistrate with respect to the Government's retention of intermingled materials.⁸⁷ Pending such a review, the majority found no reason to order the return of any property at all.⁸⁸

(3) Dissenting Opinion

The dissent began its opinion by marveling at the Government’s “breathtaking” effort to expand the “plain view” doctrine, which, according to the dissent, “clearly has no application to intermingled private electronic data.”⁸⁹ It then launched into a three-part attack on the Government’s “callous disregard” for the rights of the affected MLB players. First, the dissent noted that both DOJ guidelines and the U.S. Attorneys’ Manual discourage the use of search warrants against non-target third parties, yet the Government executed search warrants precisely because it did not want to face opposition to its grand jury subpoenas.⁹⁰

Second, the dissent observed, the Government rejected CDT’s requests for review by a U.S. Magistrate Judge – the very type of review the majority later required – and, instead, used its own preemptive review of the information to secure additional search warrants and subpoenas.⁹¹

Third, the dissent found it outrageous that the Government had threatened Quest with an obstruction of justice charge if Quest divulged the existence of the final subpoena, simply because CDT had sought to challenge the Government’s earlier subpoenas and search warrants.⁹²

After finding the district courts’ exercise of jurisdiction proper under a “callous disregard” standard, the dissent then found that those courts were correct to grant CDT’s motions, because the Government admitted that while it had no probable cause to search for and/or seize any record beyond those relating to the original 10 MLB players, its actual seizure was vastly broader.⁹³ The dissent also pilloried the majority’s proposal that a Magistrate review intermingled materials only **after** the seizure of these data **and** an aggrieved party’s objection, because affected third parties – who did not receive the search warrant – might not even know enough to object.⁹⁴ The dissent further noted that because commingling is inherent in relational databases, the majority’s holding will ensure that the Government always seizes far more data than that to which it is entitled under the warrant, thus reducing affected parties to elusive *ex post* relief.⁹⁵

In a scathing conclusion, the dissent observed that

[t]he profound consequences of the majority rule are readily demonstrated by the case at bar. Because they had no notice of the governments’s [sic] seizure, no objections were filed by the thirteen other major sports organizations, three unaffiliated business entities, and three sports competitions whose data was seized. Therefore, a magistrate will never review that unauthorized seizure under the majority holding. Under the majority’s rule, the government will also be allowed to retain all of the information it seized from those who did object because the information is co-mingled and cannot be segregated without changing its original character.⁹⁶

(4) Observations on BALCO

The BALCO majority opinion reflects a microcosm of search and seizure issues in the electronic age. It is also a cautionary tale that illustrates all too well how innocent third parties can suffer at the hands of an overreaching Government. First, BALCO demonstrates how manipulation of the means for compelling ESI – through the one-two punch of subpoenas and search warrants – effectively precluded the affected parties from challenging the scope of production or preventing the disclosure of private and privileged information.

Second, the Government’s review of data outside the scope of probable cause allowed the Government to secure additional search warrants that it could not have obtained absent the sweeping “seizure and search.” And even if the warrant could have been read to authorize the seizure of data without a showing of probable cause – which was the case for all data unrelated to the ten named MLB players – the warrant should have failed for lack of particularity. Under the majority’s standards, **any** warrant encompassing ESI in a relational database will function as a general warrant and will allow the Government to seize **all** data on the target computer system.

Third, the majority opinion leaves the searched party with no means of redress under Rule 41(g), which allows for the return of property only if (a) the search and seizure is unlawful, or (b) the searched party has a superior need for the materials seized. Under the majority’s theory, however, any warrant that authorizes the seizure of **hardware** necessarily permits a search of all **data** on that hardware. Thus, in the majority’s world, there is no “unlawful” search **or** seizure under Rule 41(g). Moreover, the Government can easily defeat the “superior need” argument by providing copies of the seized material to the searched party, which allows the Government to retain data (a) for which there was no probable cause to search or seize, and (b) was not identified with particularity in the warrant.

Finally, the majority’s proposal for *ex post* Magistrate review is of no assistance to third parties whose private information is compromised, because they may not **know** about the seizure and cannot, therefore, formally **object** to it.

Yet for all its privacy-pulverizing sweep, BALCO is not a watershed case, representing as it does merely an amalgamation of theories and standards shared among many courts that have considered the search and seizure of ESI. And because BALCO was a pre-indictment case, it did hold out some hope, however minimal, that the searched party could retrieve data beyond the scope of the search warrant before the Government used it to issue indictments. Following indictment, the standards governing the “return of property” are even stricter.

2. Post-Indictment Challenges

Although Rule 41(g) relief may be available to a criminal post-conviction,⁹⁷ an indicted party seeking to suppress the results of an unlawful search or seizure must rely on Federal Rules of Criminal Procedure 41(h) and 12.⁹⁸ Unlike a Rule 41(g) motion, a Rule 41(h) motion to suppress requires an **illegal** search or seizure, though it permits the suppression both of contraband and of items to which the movant has no legal claim of ownership.⁹⁹ Rule 41(h)/12 motions to suppress must be filed prior to trial, or the objection is waived.¹⁰⁰

While Rules 41(h) and 12 do not, themselves, specify any grounds for suppression, established case law makes clear that any relevant constitutional violation provides such grounds. In the context of ESI, that means the Fourth Amendment.¹⁰¹ Although a full examination of Fourth Amendment jurisprudence is well beyond the scope of this article, it should suffice to say that the **constitutional** dimensions of a Rule 41(g) analysis – as adumbrated above – are the same as those for a Rule 41(h) analysis.¹⁰²

Thus, where the Government obtained a warrant, the defendant bears the burden of proving an illegal search or seizure.¹⁰³ Even if the defendant proves an illegality, however, the Government may still avoid suppression by establishing facts to support the “good faith” exception to the exclusionary rule.¹⁰⁴ In the absence of a warrant, the Government must establish an exception to the warrant requirement,¹⁰⁵ just as the Government bears the burden of demonstrating voluntary consent to search.¹⁰⁶

If the defendant succeeds in his burden, or the Government fails in its, the court may suppress not only the illegally-obtained evidence, but also any subsequently-obtained evidence that derived from the primary, “tainted” evidence (the so-called “fruit of the poisonous tree”).¹⁰⁷ Before the court bars this secondary evidence, however, the Government will have an opportunity to establish one or more of the three exceptions to the exclusionary rule: independent source;¹⁰⁸ inevitable discovery;¹⁰⁹ or attenuation (“purging the taint”).¹¹⁰

Adding to the complexity of Fourth Amendment jurisprudence – based as it is on notions of “reasonableness” – is the concept of “severance,” whereby a court, in the face of a motion to suppress, can merely sever those portions of a warrant deemed constitutionally inadequate and suppress only that evidence that relates to the severed parts.¹¹¹ Thus, even facially invalid search warrants may, in part, be salvageable. (What is less clear is how the courts would order the return or suppression of intermingled data seized under the invalid portion of a warrant, in light of their seeming inability to segregate such data when overseeing the seizure of ESI.)

E. Summary

As the foregoing makes clear, a client faced with a search warrant for electronically-stored information can exercise virtually no **control** over the process, either during or after execution of the warrant. First, there is a substantial government intrusion onto the client’s property, and the client has no ability to challenge (or, God forbid, to obstruct) an ongoing search. Likewise, the client has no ability to **negotiate** the terms of the warrant before the Government seizes the client’s data.

Second, the client has no contemporaneous ability to **segregate** – and to avoid producing – irrelevant, privileged, and/or otherwise protected information that is “intermingled” with responsive data in its computer system.

Third, the client cannot **track** the seizure of ESI, unless it receives an exact copy of the information the Government seizes. Nor can the client **label** seized materials in order to track

the Government's use thereof in any continuing investigation or prosecution. Furthermore, the nature of ESI virtually ensures a broad seizure and an off-site search.

Fourth, once the information leaves the client's premises, the client has essentially no control over its use, both because existing law seems to favor broad electronic searches, and because the law provides innumerable loopholes that allow the Government to retain, and use, information outside the scope of the warrant.

Fifth, the client does not suffer alone. Third parties affected by the search and seizure may never learn of it, fail to object to it, and, possibly, suffer adverse consequences should the Government ever disclose their private data, or use it against them.

In sum, clients facing search warrants for ESI confront overwhelming odds that can keep them on the defensive throughout a government investigation (and, perhaps, a prosecution).

F. "To The Barricades:" Possible Solutions to Overly Broad Seizures¹¹²

Although there is no foolproof method for protecting your clients against the possible ravages of an ESI search warrant, there may be ways to ameliorate the pain. We address them below, in ascending order of aggressiveness.

1. DOJ's Self-Imposed Limitations

As noted in the BALCO decision, DOJ has promulgated guidelines that could, in theory, help protect clients from "third party" search warrants. These DOJ guidelines – which appear both in the Code of Federal Regulations and in the United States Attorneys' Manual – address methods for obtaining documentary materials from non-target third parties.¹¹³ The first salient principle admonishes investigators **not** to use search warrants to obtain third-party information, unless the use of a grand jury subpoena would somehow jeopardize an ongoing investigation.¹¹⁴

The second salient principle advises investigators **not** to use search warrants to obtain documentary materials from attorneys, physicians, or clergy members – where the risk of sweeping up privileged information is substantial – unless (a) the use of a subpoena would substantially jeopardize an ongoing investigation; (b) the materials sought are vital to the investigation; and (c) the investigators obtain the necessary approvals within DOJ.¹¹⁵

The third salient principle appears not in the "guidelines," but in the DOJ Manual, wherein DOJ directs Government agents to include an "explanation of the search strategy" in the affidavit accompanying the search warrant application. According to DOJ, this section of the affidavit should "explain what techniques the agents expect to use to search the computer for the specific files that represent evidence of crime and may be **intermingled** with entirely innocuous documents."¹¹⁶ As stated in the Manual, the goal of this "search strategy" section is to preempt defense arguments that Government agents "flagrantly disregarded" the warrant during execution of the search.¹¹⁷

These provisions did not, however, prevent the situation in BALCO from occurring, nor do they afford any individual any rights as against Government agents. Suffice it to say that most criminal defense attorneys would probably not feel comfortable placing the fate of their clients solely in the hands of Government investigators and prosecutors, however well-meaning these DOJ Manual principles might be.

2. The Search and Seizure Review Processes

Courts and commentators have suggested that “neutral review” of ESI could ameliorate the effects of overly broad seizures by screening out data that are privileged, beyond the scope of the warrant, or otherwise sensitive and not subject to disclosure.¹¹⁸ Possible neutral reviewers include DOJ “taint teams,” special masters, and U.S. Magistrate Judges.

“Taint teams” comprise Government agents and prosecutors who (a) are not involved in the investigation that led to the challenged search and (b) deploy a “Chinese wall” in order to avoid substantive contact with the active case agents and prosecutors.¹¹⁹ The courts are split on the value of taint teams. While taint teams purportedly have the advantage of knowledge and speed,¹²⁰ many courts have expressed discomfort with allowing the fox to guard the henhouse,¹²¹ and criminal defense lawyers are not enamored of the process, either.¹²²

“Special masters” are neutral third parties whom the court appoints to handle various (and, usually, intractable) discovery disputes.¹²³ DOJ has criticized the pace at which special masters tend to work, presumably out of concern for the time sensitivity of DOJ investigations.¹²⁴ It is unlikely, however, that criminal defense counsel would raise any objection to the use of a special master, assuming that their clients had access to the computer hardware, software, and data necessary to run their businesses while awaiting the special master’s review of seized ESI.

Although no one can reasonably quibble with the use of a U.S. Magistrate Judge to review seized data, the sheer volume of electronically-stored information in a typical computer search and seizure case makes it highly unlikely that the Magistrate would consent to undertake the task.¹²⁵ It would appear that in the BALCO case, however, the majority did not afford the Magistrate the opportunity to decline.¹²⁶ Although Magistrate review is the best outcome for the client in the current legal environment, it is also the least likely to occur, given the technological and logistical obstacles to a “filtering review” of voluminous ESI.

3. Potential Proactive Steps

a. Data Segregation

The less “aggressive” of the proactive steps – and one that clients should consider taking simply as a matter of good document management policy and procedure – is the electronic segregation of privileged data, as well as of data implicating significant privacy concerns. As a logistical matter, this may involve a number of coordinated actions, depending on how “progressive” the client is in its document management philosophy.

First, the client should prepare or update a written document retention policy that includes the management of electronically-stored information. A proper document management policy requires input and cooperation from management, in-house counsel, IT personnel, and records management personnel. At base, the client must know (a) what **types** of information it generates; (b) **where** that information is stored; (c) **how** it is stored; and (d) **who** has knowledge of the foregoing facts.

Second, the client must educate both management and employees on company policy and its implications. Training, handbooks, and human points of contact are vital, as are mechanisms for ensuring compliance with document management policies, so that the client can avoid questions about its conduct in the event of a government investigation. Notably, the destruction of data, if conducted in compliance with company policy, can save the client both money and logistical headaches and can help defeat charges of obstruction or spoliation.

Third, the client should assemble an ESI crisis management team with an emergency response plan. The team should include management, legal, IT, and accounting personnel. When a crisis – such as the receipt of a grand jury subpoena *duces tecum* or a search warrant – arises, the team should ensure immediate notice to those who know how and where the company is storing potentially relevant ESI. The team should also arrange the immediate suspension of automatic data destruction procedures and the circulation of preservation notices (a/k/a “holds”). Once it has taken these steps, the team should contact counsel and begin implementation of its crisis plan.

Finally, and most importantly, the client should consider proactive efforts to **segregate** privileged and otherwise protected data from non-privileged and routine data. Internal IT and outside consultants can address the technical feasibility of various proposals. For example, the client could store the files and e-mail of in-house counsel on a separate server to facilitate privilege review. Similarly, employees could code all privileged and protected information (such as medical records) for ease of identification in the event of a government demand for data. Even if the Government winds up seizing all of this ESI, the prior segregation will bolster the client’s position when it seeks return of the segregated data and will assist the client in crafting a post-seizure review process that maximizes its chances of preserving the sanctity of privileged and private ESI.

b. Data Encryption

The more “radical” approach to ESI “self-help” is the encryption of privileged and otherwise protected data within the client’s computers or computer network.¹²⁷ Data encryption comes in many forms, but, at base, all encryption systems require encryption codes (typically from software) and encryption keys (*e.g.*, symmetric, public, one-time pads).¹²⁸ The goal of any encryption program is to prevent unauthorized persons from accessing the client’s privileged and protected ESI. In the eyes of the client, such “unauthorized persons” may include a federal grand jury or federal law enforcement agents.¹²⁹

Let us suppose, then, that the Government has executed a search warrant at your client’s place of business and has seized both unencrypted files (*e.g.*, routine business records) and

encrypted files (*e.g.*, privileged materials and personal medical information) for off-site review. Let us further suppose that the Government could not locate, and, thus, did not seize, the key for your client's encrypted files. At this point, the Government has three options. First, it can send the client's encrypted data to its super-computer-equipped laboratories and endeavor to break the encryption, which, depending on the encryption method utilized, could be extraordinarily difficult and time-consuming.¹³⁰

Second, the Government can serve a grand jury subpoena demanding production of the key, either by way of testimony or by way of physical production of a document containing the key. The result of this endeavor will depend on the status of the client. If the client is an individual, she may assert a Fifth Amendment right to refuse to divulge the key, either orally or in writing.¹³¹

With respect to an **oral** disclosure, there is, to the best of the author's knowledge, no legal precedent that would require the client to testify against herself under these circumstances. In fact, one recent case specifically upheld an individual's right to withhold a computer drive encryption password from the Government, on the grounds that disclosure of the password would (a) reflect the individual's thoughts and (b) demonstrate control over, knowledge of, and the authenticity of, the potentially incriminating information within the computer drive.¹³² With respect to the **written** disclosure of a pre-existing document embodying the key, the individual client should enjoy "act of production" immunity, under the same rationale applicable to an oral disclosure.¹³³ At a minimum, an individual client has a powerful Fifth Amendment argument against a subpoena that seeks her encryption key.¹³⁴

If the client is not an individual, but a legal entity, it has no Fifth Amendment rights and cannot, therefore, refuse to comply with the subpoena.¹³⁵ Indeed, the U.S. Supreme Court has rather emphatically denied Fifth Amendment protection to corporate business records.¹³⁶ But all is not lost. If the Government serves a subpoena for production of the encryption key, the corporate client may negotiate with the Government regarding the withholding of privileged materials and/or move to quash the subpoena under Rule 17.¹³⁷ By doing so, the client will have secured at least some level of *ex ante* review, an outcome it could not have achieved if the Government had simply seized all of its unencrypted computer data pursuant to a broad search warrant. The existence of the subpoena may also provide third parties with notice and an opportunity to object to the compelled disclosure of **their** protected information, a situation that did not obtain – to the great detriment of such third parties – in the BALCO case.¹³⁸

Third, even if the Government never serves a subpoena, it can still negotiate with the client, or with you, over an appropriate protocol for a search of the client's ESI. Having gone through the dual processes of segregation and encryption, the client will be in an excellent position to establish that the encrypted information is protected from disclosure and to insist that, to the extent the Government wants proof of that protected status, the client will produce the data only to a neutral third party for review. In this manner, the client may achieve through encryption that which it could not achieve through Rule 41 or through the Fourth Amendment to the United States Constitution.¹³⁹

III. CONCLUSION

Times have changed, but the rules of the game have not. In the digital age, for reasons both legal and logistical, clients whose premises are searched will quickly lose control over their ESI, including irrelevant and/or protected information that should not be in the hands of the Government, however well-meaning its agents may be. The problem is compounded for third parties, who may never know of the search and will, therefore, have no ability to protect their confidential information, as the BALCO case amply demonstrates.

There is no perfect solution to this situation. The case law is not developing in the right direction, and Congress has yet to act to prevent this creeping invasion of our cherished privileges and protections. But is all resistance therefore futile? Might not careful ESI management, the judicious use of existing technology, and *ex ante* appeals to the courts interpose at least some obstacle to the wholesale seizure of our clients' protected data? Can self-help level the playing field in what is now a lopsided game? Although the Government's power in this area is undeniably vast, we are not without arrows in our quivers. This article, it is hoped, will assist you in deciding which ones to fit to your bow.

¹ FED. R. CRIM. P. 17(c) (2007).

² The U.S. Supreme Court has described the grand jury as a “grand inquest, a body with powers of investigation and inquisition, the scope of whose inquiries is not to be limited narrowly by questions of propriety or forecasts of the probable result of the investigation.” *Blair v. United States*, 250 U.S. 273, 282 (1919). *See also United States v. R. Enters., Inc.*, 498 U.S. 292, 297 (1991) (holding that the grand jury may “inquire into all information that might possibly bear on its investigation until it has identified an offense or has satisfied itself that none has occurred”).

³ *See Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 208-09 (1946).

⁴ *See, e.g., In re Grand Jury Proceedings*, 115 F.3d 1240, 1244 (5th Cir. 1997) (holding that “there is no probable cause requirement for the issuance of a grand jury subpoena [, because i]ssues of probable cause relate solely to the validity of [a] search warrant”); *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 854 (9th Cir. 1991) (finding that “[s]ubpoenas are not search warrants, [because t]hey involve different levels of intrusion on a person’s privacy . . . [and] the person served with a subpoena determines whether he will surrender the items identified in the subpoena or challenge the validity of the subpoena prior to compliance”).

⁵ *See, e.g., In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (observing that the Supreme Court’s holdings on the overbreadth of subpoenas *duces tecum* suggested that any restrictions imposed “rest[ed] not on the Fourth Amendment but on the less rigid requirements of the due process clause”); *cf. United States v. Dionisio*, 410 U.S. 1, 9 (1973) (holding that a personal appearance subpoena requiring production of a voice exemplar was not a “seizure” under the Fourth Amendment); *United States v. Mara*, 410 U.S. 19, 21 (1973) (reaching the same conclusion with respect to a handwriting exemplar).

⁶ *Branzburg v. Hayes*, 408 U.S. 665, 708 (1972). See also *R. Enters., Inc.*, 498 U.S. at 299 (finding that grand juries “are not licensed to engage in arbitrary fishing expeditions, nor may they select targets of investigation out of malice or intent to harass”); *In re Grand Jury Subpoenas 04-124-03 and 04-124-05*, 454 F.3d 511, 519 (6th Cir. 2006) (holding that “grand juries are not empowered to override private rights in all cases” and that “grand juries may not use their investigatory authority ‘to violate a valid privilege, whether established by the Constitution, statutes, or the common law’”); *In re Grand Jury*, 286 F.3d 153, 159 (3d Cir. 2002) (noting that the courts have “some authority to limit the grand jury’s power” but finding that intervenors could not protect evidence in their civil lawsuit from production in response to a grand jury subpoena *duces tecum*).

⁷ See, e.g., *R. Enters., Inc.*, 498 U.S. at 299; *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950) (finding an administrative subpoena to be valid where the commanded production was “not too indefinite” and the information sought was “reasonably relevant”).

⁸ See, e.g., *In re Grand Jury Proceedings*, 857 F.2d 707, 709 (10th Cir. 1988); *In re Horowitz*, 482 F.2d at 79.

⁹ *R. Enters., Inc.*, 498 U.S. at 301 (holding that “the burden of showing unreasonableness must be on the recipient who seeks to avoid compliance” and that a subpoena will be upheld unless “there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation”); *In re Grand Jury Proceedings*, 857 F.2d at 709 (holding that a subpoena is valid in all but the “clearest case of abuse”).

¹⁰ See, e.g., *Morton Salt Co.*, 338 U.S. at 653; *In re Subpoena Duces Tecum*, 228 F.3d 341, 349 (4th Cir. 2000).

¹¹ In addition, counsel may negotiate the **format** of any production, because production format – e.g., native file, TIFF, PDF – affects the client’s ability to control and to track its production. For example, metadata that appear in a native file format will not appear in a PDF format. Moreover, TIFF and PDF productions are easier to control, because the client can Bates-number individual pages, and no recipient of the production can alter the documents without detection. A full discussion of the implications of format choice – including cost – is well beyond the scope of this article.

¹² Especially in the context of ESI productions, counsel are likely to employ search filters to screen out potentially privileged materials. Although such filters – typically incorporating the identities of all in-house and outside counsel to the subpoena recipient – tend to be over-inclusive on the first pass, they are only as good as the search terms they employ, and they may, in fact, miss some privileged materials. As such, while the use of search filters can expedite the provision of responsive documents, they are no guarantee against the inadvertent production of privileged information.

¹³ See Dan K. Webb, Robert W. Tarun, and Steven F. Molo, CORPORATE INTERNAL INVESTIGATIONS §606[2], at 6-36.4 (Law J. Press 2003) (citing cases finding waiver and cases rejecting waiver and noting that “following the modern trend, some courts have taken a less strict approach and have examined the intent of the party who is claimed to have waived the privilege”); see also *Ciby-Geigy Corp. v. Sandoz Ltd.*, 916 F. Supp. 404, 410-11 (D. N.J. 1995) (explaining the “modern” approach to inadvertent waiver as an analysis that considers precautionary measures taken to avoid disclosure, the speed of the effort to recover disclosed materials, the scope of discovery, the extent of the disclosure, and equitable considerations); *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) (same); *Harp v. King*, 835 A.2d 953, 966 (Conn. 2003) (applying and discussing the five factors); *Elkton Care Ctr. Assocs., Ltd. P’ship v. Quality Care Mgmt., Inc.*, 805 A.2d 1177, 1185 (Md. Ct. Spec. App. 2002) (same). This “modern” approach is now the majority rule. See John K. Villa, *Inadvertent Disclosure of Privileged Material: What is the Effect on the Privilege and the Duty of Receiving Counsel?*, ACC DOCKET, Oct. 2004, at 108, 110.

¹⁴ See Proposed FED. R. EVID. 502, as set forth in S. 2450, 110th Cong. (2007). Subsection (b) of the proposed Rule provides that the inadvertent production of privileged materials in a federal matter does not operate as a waiver of privilege in any federal or state proceeding, if the privilege holder took “reasonable precautions to prevent disclosure” and “reasonably prompt measures” to recover the materials after learning of the inadvertent disclosure. *Id.* The Judicial Conference of the United States approved the measure and forwarded it to Congress, where Sen. Patrick Leahy (D. Vt.), Chair of the Senate Judiciary Committee, introduced pertinent legislation on December 11, 2007. Pursuant to 28 U.S.C. §2074(b), Congress must approve any rule, such as Rule 502, that creates, abolishes, or modifies an evidentiary privilege. See U.S. Courts, Federal Rulemaking, Bill Introduced to Enact Evidence Rule 502: 12/11/07, <http://www.uscourts.gov/rules/index2.html#ev502bill> (last visited Jan. 14, 2008).

¹⁵ On a separate but related note, proposed Rule 502 would also permit the “selective waiver” of privileges in the context of a government investigation. In a nutshell, proposed Rule 502 would allow a subpoenaed party, as part of its cooperation in a federal government investigation, to disclose privileged materials to the Government, without fear of waiving its privileges in other forums, such as related civil litigation, as long as a federal court entered an order to that effect. See Proposed FED. R. EVID. 502(d).

¹⁶ See, e.g., *In re Grand Jury Subpoena Duces Tecum Addressed to Corrado Bros, Inc.*, 367 F. Supp. 1126, 1132 (D. Del. 1973) (holding that “[o]nly in the most extreme case of a clear showing of unreasonableness, of Government abuse of power, will the Court be induced to quash an otherwise valid grand jury subpoena on the basis that it was overly burdensome”).

¹⁷ See FED. R. CRIM. P. 17(c); see also *R. Enters., Inc.*, 498 U.S. at 299 (noting that Rule 17(c) allows the court to modify a subpoena if compliance would be “unreasonable or oppressive”); *In re Grand Jury*, 111 F.3d 1066, 1075 (3d Cir. 1997) (finding that the courts are empowered to

quash or modify grand jury subpoenas under Rule 17(c)); *In re Subpoena to Testify Before Grand Jury Numbered S286-4-7*, 630 F. Supp. 235, 237 (N.D. Ind. 1986).

¹⁸ See, e.g., *In re Horowitz*, 482 F.2d at 79-80 (limiting the time period covered to 7 years, rather than the 23 years listed in the subpoena); *In re Subpoena to Testify*, 630 F. Supp. at 237-38 (excising all categories of documents other than those specifically enumerated following the “included but not limited to” clauses of the subpoena); *In re Grand Jury Subpoena Duces Tecum Addressed to Provision Salesmen and Distribs. Union*, 203 F. Supp. 575, 580 (S.D.N.Y. 1961) (reducing the time period of the subpoena from 18 years to 10 years).

¹⁹ See *United States v. Hubbell*, 530 U.S. 27, 36-37 (2000) (recognizing the “act of production” doctrine in Fifth Amendment jurisprudence); *United States v. Doe*, 465 U.S. 605, 612 (1984) (noting that the “act of production” doctrine applies to documents not otherwise privileged under the Fifth Amendment but which might have an incriminating effect if produced); see also *Doe v. United States*, 487 U.S. 201, 209 (1988) (finding that the privilege against self-incrimination protects a suspect from being compelled to disclose any knowledge he has or to speak his own guilt, such as by admitting, even implicitly, that evidence exists, is authentic, or is within the suspect’s control).

²⁰ See, e.g., *United States v. Plunk*, 153 F.3d 1011, 1020 (9th Cir. 1998); *In re Grand Jury*, 111 F.3d at 1073-74; *United States v. Phibbs*, 999 F.2d 1053, 1077 (6th Cir. 1993); *In re Grand Jury Proceedings*, 814 F.2d 61, 66 (1st Cir. 1987); *United States v. Raineri*, 670 F.2d 702, 712 (7th Cir.), *cert. denied*, 459 U.S. 1035 (1982).

²¹ See *supra* note 11.

²² See FED. R. CRIM. P. 41(a)(2)(A) (including “information” in its definition of “property subject to search or seizure”).

²³ See FED. R. CRIM. P. 41(b).

²⁴ See FED. R. CRIM. P. 41(c)(1). The remaining types of “property” subject to search and seizure are contraband, fruits of a crime, “other items illegally possessed,” and “property designed for use, intended for use, or used in committing a crime” (the so-called “instrumentalities” of crime). See FED. R. CRIM. P. 41(c)(2)&(3).

²⁵ See FED. R. CRIM. P. 41(d)(1).

²⁶ See FED. R. CRIM. P. 41(e)(2).

²⁷ See generally FED. R. CRIM. P. 41. Although the Rule does not specify the **order** in which a “search and seizure” must occur, the language of the Rule strongly suggests that the “typical” scenario is one in which federal agents “search for” specified property, **then** “seize” it. See, e.g., FED. R. CRIM. P. 41(b)(1) (stating that the Magistrate can issue a warrant to “search for and seize

. . . property”); (d)(1) (allowing a warrant to issue on probable cause to “search for and seize . . . property”); (e)(2) (stating that the warrant must “identify the . . . property to be searched [and] identify any . . . property to be seized”). In short, within Rule 41, the “search” always **precedes** the “seizure.”

²⁸ See U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (July 2002), available at <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm> (hereinafter “DOJ Manual”).

²⁹ See *id.* at 29-30 & 42; see also Forward Edge II, *Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers Provided by the U.S. Department of Justice* 4, <http://www.forwardedge2.usss.gov/fieldGuide/formsAndGoBys.aspx>.

³⁰ U.S. Const., amend. IV.

³¹ *E.g.*, *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J. concurring); see also *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (holding that a Fourth Amendment “search” occurs “when an expectation of privacy that society is prepared to consider reasonable is infringed” and that a “seizure” occurs when the government “meaningfully interferes with an individual’s possessory interests in property”).

³² Wright, King & Klein, *FEDERAL PRACTICE AND PROCEDURE: CRIMINAL* 3D §662, at 45 (Thompson West 2004) (citing cases for the “probable cause” standard) (hereinafter “FEDERAL PRACTICE AND PROCEDURE”).

³³ *E.g.*, *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (holding that probable cause is established if the evidence presented to the magistrate allows him to conclude that there is a “fair probability that contraband or evidence of a crime will be found in a particular place”); *United States v. Infante-Ruiz*, 13 F.3d 498, 502 (1st Cir. 1994) (explaining that “probable cause” does not mean “certainty”).

³⁴ See *Gates*, 462 U.S. at 272 (confirming the use of the “totality-of-the-circumstances” test); *Andresen v. Maryland*, 427 U.S. 463, 478 n.9 (1976) (upholding the validity of a search warrant based on information that was three months old, where the evidence suggested that the materials would still exist at the time of the proposed search).

³⁵ See *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (holding that “[b]y limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justification, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit”); *United States v. Ross*, 456 U.S. 798, 824 (1982) (holding that the scope of a lawful search is “defined by the object of the search and the places in which there is probable cause to believe that it may be found”).

³⁶ See *Steele v. United States*, 267 U.S. 498, 503 (1925) (holding that the Fourth Amendment requires that the place to be searched and the items to be seized be described with particularity so as to leave “nothing . . . to the discretion of the officer executing the warrant”); see also *Marron v. United States*, 275 U.S. 192, 196 (1927) (holding that the agents should have no discretion as to what they seize during a search); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (noting that the purpose of the particularity requirement is to prevent the Government from engaging in exploratory rummaging through an individual’s personal property).

³⁷ See Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 YALE J. L. & TECH. 120, *2 (2007) (explaining the history of “general warrants,” “writs of assistance,” and the desire of the Framers to avoid these abuses through the Fourth Amendment); G. Robert McLain, Jr., *Casenote: United States v. Hill: A New Rule, But No Clarity For the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1075 (2007) (same).

³⁸ See, e.g., *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (holding that government agents must specify in their warrant application what type of files they seek to search and seize); *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041 (S.D.N.Y. April 4, 2007) (holding that “when the government seeks to seize the information stored on a computer, as opposed to the computer itself, that underlying information must be identified with particularity and its seizure independently supported by probable cause”); DOJ Manual, *supra* note 28, at 42 (advising that if probable cause for a computer search relates only to the information contained therein, “the warrant should describe the information, rather than the physical storage device which happens to contain it”).

³⁹ See, e.g., *United States v. Riccardi*, 405 F.3d 852, 862-63 (10th Cir. 2005) (invalidating a warrant that authorized the seizure of the defendant’s computer and digital media but did not specify the nature of the materials that the agents were authorized to examine); *United States v. Bianco*, 998 F.2d 1112, 1116 (2d Cir. 1993) (holding that a warrant lacked particularity where it did not describe the possible crimes involved and contained a “catch-all” provision allowing seizure of “any and all records” of a certain type); *United States v. Hunter*, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (holding that a portion of a search warrant seeking “all” computers, storage devices, and software was an invalid “catch-all” provision that violated the Fourth Amendment’s particularity requirement); *Matter of Search Warrant for K-Sports Imports, Inc.*, 163 F.R.D. 594, 596 (C.D. Cal. 1995) (holding that the use of “including but not limited to” language converted a search warrant into an unlawful “general warrant”); *United States v. Clough*, 246 F. Supp. 2d 84, 87 (D. Me. 2003) (striking down a warrant that contained no reference to the alleged crimes and no meaningful limitations on the scope of a computer search); cf. *Groh v. Ramirez*, 540 U.S. 551, 559 (2004) (holding that “[t]he uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional”).

⁴⁰ See, e.g., *United States v. Adjani*, 452 F.3d 1140, 1148 (9th Cir. 2006) (finding that the warrant was as particular as could reasonably be expected given the nature of the alleged crimes at issue);

United States v. Upham, 168 F.3d 532, 535 (1st Cir.), *cert. denied*, 527 U.S. 1011 (1999) (finding the seizure, and subsequent search, of a computer and all data disks in the defendant's former residence to be "about the narrowest definable search and seizure reasonably likely to obtain the [child pornography] images"); *United States v. Hall*, 142 F.3d 988, 996 (7th Cir. 1998) (upholding the seizure, and subsequent search, of all hardware and software that could be used to store child pornography).

⁴¹ Trepel, *supra* note 37, at *4.

⁴² *See, e.g., United States v. Fleet Mgmt. Ltd.*, -- F. Supp. 2d --, 2007 WL 3146674 (E.D. Pa. Oct. 29, 2007) (finding it "plainly insufficient to identify the computer hard drives with particularity as the hard drives were merely the property to be searched, not the property to be seized"); *In the Matter of the Search of 3817 W. West End, First Floor, Chicago, Illinois 60621*, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) (noting the anomaly of agents "seizing" computer equipment **before** they actually "search" it for information identified in the warrant); *see also* Orin Kerr and Susan Brenner, *Search and Seizure in a Digital World?*, LEGAL AFFAIRS DEBATE CLUB, August 8, 2005, at 4-5, http://www.legalaffairs.org/webexclusive/debateclub_searchseizure0805.msp (positing that even if the Government only **copies** computer data, it has "seized" it, because it has deprived the owner of the exclusive right to its use, and that there can be no "search" of computer data until a human being actually examines it); Orin Kerr, *Search and Seizure in a Digital World*, 119 HARV. L. REV. 531, 551 (2005) (arguing that computer data is "searched" only when a human being can perceive it).

⁴³ DOJ Manual, *supra* note 28, at 28 (emphasis added).

⁴⁴ McLain, *supra* note 37, at 1091-92.

⁴⁵ *Id.* at 1092-93. *See also Upham*, 168 F.3d at 537 (observing that "until the deleted information is actually overwritten by new information, the old information can often be recovered").

⁴⁶ *See, e.g., 3817 W. West End*, 321 F. Supp. 2d at 958 (observing that computers typically "intermingle" relevant documents with those for which the Government has no probable cause to search).

⁴⁷ *See Kerr, supra* note 42, at 556 (noting that in a networked world, a "single physical storage device can store the private files of thousands of different users").

⁴⁸ *See, e.g., Adjani*, 452 F.3d at 1149 (upholding the seizure and search of all computers on the premises where the alleged crimes were specified in the warrant); *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) (upholding the seizure of an entire computer system, even though the warrant did not specify the crime under investigation, where the agents knew that a third party had sent child pornography to the defendant's computer); *Upham*, 168 F.3d at 535; *Hall*, 142 F.3d at 996; *United States v. Scott-Emuakpor*, 1:99-CR-138, 2000 WL 288443, at *7-8 (W.D. Mich. Jan. 25, 2000) (finding no Fourth Amendment violation where the agents seized all

computer hardware and software, even though the warrant identified a limited set of data to be seized); *United States v. Lamb*, 945 F. Supp. 441, 458 (N.D.N.Y. 1996) (authorizing the seizure of all computer files, even though the warrant was for child pornography images only, where the executing agents could not determine the content of any given file until they examined it); *United States v. Gawrysiak*, 972 F. Supp. 853, 861 (D. N.J.), *aff'd*, 178 F.3d 1281 (3d Cir. 1999) (finding no Fourth Amendment violation where the agents copied all of the defendant's computer files while searching for evidence of a fraud scheme, because the defendant's business dealings were "pervaded" by fraud).

⁴⁹ See, e.g., *United States v. Hill*, 459 F.3d 966, 977-78 (9th Cir. 2006) (finding any requirement of a search protocol to be unreasonable, because criminals can easily manipulate ESI to avoid detection, and holding that "[t]here is no way to know what is in a file without examining its contents"); *United States v. Brooks*, 427 F.3d 1246, 1252 (10th Cir. 2005) (finding no Fourth Amendment violation where the warrant did not specify a search methodology for computer data); *Upham*, 168 F.3d at 537 (holding that the warrant process is concerned only with identifying **what** is to be searched and seized, not **how**); *United States v. Kaechele*, 466 F. Supp. 2d 868, 897 (E.D. Mich. 2006) (finding no support in the case law for a requirement that the Government employ a narrowly-tailored search methodology); cf. *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 651-52 (1995) (stating that for search methods not in existence when the Fourth Amendment was adopted, the only constitutional test is "reasonableness"); *Dalia v. United States*, 441 U.S. 238, 257 (1979) (holding that "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant").

⁵⁰ See, e.g., *Hill*, 459 F.3d at 978; Kerr, *supra* note 42, at 571 (describing the *ex ante* search protocol approach as "deeply flawed," because "the forensics process is too contingent and unpredictable for judges to establish *ex ante* rules"), 575 (asserting that Magistrates are "poorly equipped to evaluate whether a particular search protocol is the fastest and most targeted way of locating evidence stored on a hard drive"); Trepel, *supra* note 37, at *6 (opining that, due to differences in operating systems and software, as well as conscious efforts by criminals to hide data, an agent cannot know "which forensic tool is best suited to her search until she begins her examination of the files"); cf. *United States v. Wuagneux*, 683 F.2d 1343, 1349 (11th Cir. 1982) (finding that warrant execution requires "practical flexibility" in complex white collar cases, including fraud).

⁵¹ See, e.g., *Hill*, 459 F.3d at 978 (opining that "[f]orcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white substance if it is labeled 'flour' or 'talcum powder'"); *Vilar*, 2007 WL 1075041, at *38 (stating that "it seems manifestly obvious that any requirement that a computer search be confined by a key-word search protocol would inevitably immunize criminals . . . [because it] would of necessity leave out any encoded documents, or any documents that used acronyms or other abbreviations in place of the 'key words'").

⁵² See, e.g., *Upham*, 168 F.3d at 535 (finding that, “[a]s a practical matter, the seizure and subsequent off-premises search of the [defendant’s] computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the [identified pornographic] images”); *United States v. Maali*, 346 F. Supp. 2d 1226, 1246-47 (M.D. Fla. 2004) (approving a seizure and off-site search, despite the fact that many non-responsive documents were undoubtedly stored on the seized computers).

⁵³ See DOJ Manual, *supra* note 28, at 32 (noting DOJ’s preference for off-site searches, due to the enormous amounts of data computers hold; the logistics of retrieving mislabeled, encrypted, hidden, and deleted files; practical limitations on the time agents can spend in a target’s home or business; and the risk of damage to the data to be seized if removal or copying is not done with the proper forensic tools); see also *McLain*, *supra* note 37, at 1083-84 (noting that on-site examination of data can be intrusive to the target and can risk alteration or destruction of the data, if not done in a forensically-sound manner).

⁵⁴ See DOJ Manual, *supra* note 28, at 48.

⁵⁵ See, e.g., DOJ Manual, *supra* note 28, at 32 (criminals may “booby-trap” their computers, such that any effort to retrieve data leads to its destruction), 49 (noting that criminals frequently mislabel or hide files, configure data in confusing ways, employ code words to escape detection, and encrypt their ESI, all in an effort to frustrate the Government’s efforts to obtain responsive electronic information); *Trepel*, *supra* note 37, at *6 (noting the difficulty of *ex ante* protocols when criminals endeavor to prevent discovery of electronic evidence); *McLain*, *supra* note 37, at 1092-93 (stating that suspects may attempt to conceal ESI in a number of ways, including deleting files, hiding evidence in inaccessible areas of the hard drive, or concealing data within other files, such as through encryption or steganography (the embedding of text files in photographic files)).

⁵⁶ See, e.g., *Horton v. California*, 496 U.S. 128, 136 (1990) (setting forth the requirements of the doctrine, to include (a) the property was in plain view; (b) the property’s incriminating character was immediately apparent; (c) the officer was lawfully in the position from which he made the plain view sighting; and (d) the officer had probable cause to believe the property was subject to seizure); FEDERAL PRACTICE AND PROCEDURE §668.1, at 190, 195 (discussing the elements of the plain view doctrine and its development in the law).

⁵⁷ See, e.g., *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003) (upholding the plain view seizure of child pornography during the search of a computer for evidence relating to the murder of the defendant’s girlfriend); *United States v. Walser*, 275 F.3d 981, 986-87 (10th Cir. 2001) (finding no Fourth Amendment violation where the officer searching for evidence of drug distribution discovered child pornography and secured a separate warrant to continue his search); *United States v. Gray*, 78 F. Supp. 2d 524, 528-29 (E.D. Va. 1999) (upholding a plain view seizure where the agent came across evidence of child pornography while lawfully searching for evidence of computer hacking); *Commonwealth v. Hinds*, 768 N.E.2d 1067, 1072-73 (Mass. App. Ct. 2002) (upholding the plain view seizure of child pornography where the officer, while

searching for identified electronic mail, observed salaciously-titled files that gave him probable cause to open the additional files and confirm their pornographic content). *But see Carey*, 172 F.3d at 1273 (denying a plain view seizure where the officer came upon evidence of child pornography while searching for evidence of drug distribution, then continued to open files that were clearly child pornography without seeking another warrant to expand the scope of his search); *United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996) (reversing the defendant's conviction of certain crimes based on the seizure of alleged plain view evidence where the investigators were not lawfully searching the email files at issue, because the "screen name" that they were searching was not set forth in the warrant).

⁵⁸ *See Carey*, 173 F.3d at 1273; *Maxwell*, 45 M.J. at 422.

⁵⁹ *See* FED. R. CRIM. P. 41(g) (2007). The Rule further provides that (a) the court must take evidence on any issue necessary to disposition of the motion, and (b) if the court orders property returned, it may impose conditions to protect the Government's access to the property for use in "later proceedings." *Id.*

⁶⁰ *E.g., In re Grand Jury Investigation Concerning Solid State Devices, Inc.*, 130 F.3d 853, 855-56 (9th Cir. 1997); *Klitzman, Klitzman and Gallagher v. Krut*, 744 F.2d 955, 962 (3d Cir. 1984) (ordering the return of law office files where the seizure was overly broad, the attorney-client privilege was violated, and the law firm was deprived of files it needed to conduct its business); *Watts v. Kroczyński*, 636 F. Supp. 792, 800-02 (W.D. La. 1986) (ordering the return of property seized outside the scope of the warrant).

⁶¹ *See United States v. Leon*, 468 U.S. 897, 928 (1984) (establishing the "good faith" exception to the exclusionary rule).

⁶² *See, e.g., James v. Illinois*, 493 U.S. 307, 311-14 (1990) (allowing the Government to use illegally-seized evidence for purposes of impeachment and rebuttal); *United States v. Havens*, 446 U.S. 620, 626-28 (1980) (permitting the Government to use illegally-seized evidence to impeach witnesses at trial); *Rakas*, 439 U.S. at 139-40 (holding that illegally-seized evidence may be used against third parties who were not "aggrieved" by the Fourth Amendment violation); *United States v. Calandra*, 414 U.S. 338, 354 (1974) (allowing the Government to use illegally-seized evidence when questioning witnesses before the grand jury).

⁶³ *See Calandra*, 414 U.S. at 349 n.6 (stating that Rule 41(e), the predecessor to Rule 41(g), "does not constitute a statutory expansion of the exclusionary rule"); *United States v. Roberts*, 852 F.2d 671, 675 (2d Cir. 1988) (holding that Rule 41 is subject to any exceptions to the exclusionary rule).

⁶⁴ This aspect of Rule 41 looms large in cases where the aggrieved person is a third party not suspected of any wrongdoing. *See* FEDERAL PRACTICE AND PROCEDURE §673, at 337 (noting that the Supreme Court, in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), upheld the use of search warrants against non-target third parties).

⁶⁵ See, e.g., *United States v. Marolf*, 173 F.3d 1213, 1219 (9th Cir. 1999) (holding that motions for the return of property are treated as equitable proceedings where no charges are pending against the movant); *United States v. Dean*, 80 F.3d 1535, 1542 (11th Cir. 1996) (stating that a motion for return of property is an equitable proceeding undertaken only in exceptional cases where equity demands the court's intervention); *In re Matter of the Search of Kitty's East*, 905 F.2d 1367, 1370-71 (10th Cir. 1990) (stating the requirements of irreparable injury and inadequate remedy at law); *In re Certain Pharmaceuticals and Proceedings of Northland Providers, Inc.*, 78 F. Supp. 2d 954, 960 (D. Minn. 1990) (describing a Rule 41 motion brought by an unindicted person as a "suit in equity," rather than as a motion under the Federal Rules of Criminal Procedure); FEDERAL PRACTICE AND PROCEDURE §673, at 353 (setting forth the requirements of irreparable injury and inadequate remedy at law). Some Circuits have also required the movant to prove that the Government acted with "callous disregard" for the movant's constitutional rights during the questioned search or seizure. See, e.g., *In re Search of Law Office, Residence, and Storage Unit of Alan Brown*, 341 F.3d 404, 409 (5th Cir. 2003). As noted earlier, these standards do not apply when the search or seizure was itself illegal under the Fourth Amendment. See *Application of First United Financial Corp. for Return of Seized Property*, 620 F. Supp. 1450, 1452 (E.D.N.Y. 1985).

⁶⁶ E.g., *Ramsden v. United States*, 2 F.3d 322, 326 (9th Cir.), cert. denied, 511 U.S. 1058 (1994).

⁶⁷ See, e.g., *Offices of Lakeside Non-Ferrous Metals, Inc. v. United States*, 679 F.2d 778, 780 (9th Cir. 1982) (holding that the court must balance the hardship to the movant from the loss of his property against the Government's interest in maintaining control of the property); *United States v. Premises Known as 608 Taylor Ave.*, 584 F.2d 1297, 1304 (3d Cir. 1978) (describing the balancing test); *In re Grand Jury Subpoena Duces Tecum Issued to Roe & Roe, Inc.*, 49 F. Supp. 2d 451, 453 (D. Md. 1999) (noting that courts must balance the Government's need for the property with the owner's right to use that property); *Matter of Search Warrant for Premises Known as Encore House*, 100 F.R.D. 700, 704 (S.D.N.Y. 1983) (ordering the return of seized checks where the Government's retention thereof would render them uncollectible and where there was inadequate proof that the checks were the fruits of a crime).

⁶⁸ DOJ Manual, *supra* note 28, at 53.

⁶⁹ See, e.g., *Standard Drywall, Inc. v. United States*, 668 F.2d 156, 157 n.2 (2d Cir. 1982) (expressing doubt that a movant could ever show irreparable harm, other than with respect to privileged documents, where the Government returns originals and keeps copies, or vice versa); *In the Matter of the Search of 5444 Westheimer Road Suite 1570, Houston, Texas on May 4, 2006*, Misc. Action No. H-06-238, 2006 U.S. Dist. Lexis 48850, at *7 (S.D. Tex. July 6, 2006) (denying a Rule 41(g) motion where, among other things, the Government had already provided the movant with copies of the privileged documents at issue). On the other hand, if the Government can work from copies of the seized materials, the court may order the return of the movant's originals. See *Johnson v. United States*, 971 F. Supp. 862, 869 (D. N.J. 1997) (noting that the courts typically allow the Government to retain copies of illegally seized evidence, even

when the movant is successful in obtaining a return of the materials); *United States v. Bryant*, No. 95Cr240(JFK), 1995 WL 555700, at *3 (S.D.N.Y. Sept. 18, 1995) (ordering the return of computers where the movant needed them to run his business and the Government had copies of the relevant data).

⁷⁰ See *Johnson v. United States*, 971 F. Supp. at 868 (denying a Rule 41 motion where the aggrieved party was not an ongoing enterprise and, thus, had no need of its computer tapes); *K-Sports Imports*, 163 F.R.D. at 597 (denying a Rule 41 motion where the computer records were subject to a civil forfeiture proceeding). Of course, if the Government no longer has a plausible need for the seized materials, the court may order them returned. See *United States v. Moore*, 188 F.3d 516, 1999 WL 650568, at *6 (9th Cir. July 15, 1999) (ordering return of a convicted defendant's computer where the Government had "ample opportunity to download or otherwise copy whatever material is on [it]") (unpublished opinion); *United States v. Jones*, 42 F. Supp. 2d 615, 617 (W.D.N.C. 1999) (finding that the return of seized property is appropriate where the Government no longer needs the property, it is not subject to forfeiture, and the defendant is entitled to lawful possession of it).

⁷¹ *Comprehensive Drug Testing, Inc.*, 473 F.3d at 920.

⁷² *Id.* at 920-21.

⁷³ *Id.* at 921.

⁷⁴ *Id.* at 922-23. The FBI also used information obtained during the CDT search to request a third search warrant, this one for records that another group of agents was unable to find during its search of Quest, because the records they found bore only identification numbers, not the names of the players whose test results the Government sought in its earlier search warrant. *Id.*

⁷⁵ *Id.* at 923-24.

⁷⁶ *Id.* at 924-25.

⁷⁷ *Id.* at 924. Specifically, the Nevada judge found that the Government had "callously disregarded the affected players' constitutional rights" and had unreasonably refused to comply with the procedures set forth in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), with regard to the search and seizure of "intermingled" records. *Id.* The California judge further rejected the Government's argument that its seizure of information regarding additional athletes fell under the "plain view" exception to the warrant requirement. *Id.*

⁷⁸ *Id.* at 925-26.

⁷⁹ *Id.* at 926. This holding is of interest to us only insofar as it confirms that where an individual has a reasonable expectation of privacy in ESI seized from a third party, that individual has standing to contest the search and seizure.

⁸⁰ *See id.* at 929 (noting that the Government had conceded that the movants had no adequate remedy at law), 936 (concluding that the players possessed “strong privacy interests” in both their specimens and their drug testing results and that the players would likely suffer irreparable injury if the results of their drug screens were publicly disclosed).

⁸¹ *Id.* at 936.

⁸² *Id.* at 930-32. While addressing this issue, the majority made a number of interesting observations about the Government’s use of its power to demand the production of ESI. First, the majority observed that “while a subpoena may be quashed, a ‘person to be searched has no lawful way to prevent execution of the warrant.’” *Id.* at 930 n.30 (quoting *In re Grand Jury Subpoena Dated December 10, 1987*, 926 F.2d 847, 854 (9th Cir. 1991)). Rather, any remedy for a Fourth Amendment violation will be *ex post*, through Rule 41(g) or Rule 12. *Id.* Second, the majority adverted to the fact that the Government’s conduct violated its own standards, set forth in the DOJ Manual, which strongly discourage the use of search warrants with regard to non-target third parties. *Id.* at 930 n.31.

⁸³ *Id.* at 932-34. As the majority put it, “the agents did not remove files without a relation to the Balco investigation,” and their decision to remove files from the premises “stemmed not from disregard of privacy rights, but from sensitivity to the ongoing disruption caused by the search.” *Id.* at 934.

⁸⁴ *Id.* at 935.

⁸⁵ *Id.* at 937.

⁸⁶ *Id.*

⁸⁷ *Id.* at 938. Specifically, the majority held that “while the government may seize intermingled data for off-site review to minimize intrusiveness of a computer search, it may not retain or use the evidence after proper objections are raised, unless a magistrate subsequently reviews and filters the evidence off-site.” *Id.* at 940.

⁸⁸ *Id.* at 940.

⁸⁹ *Id.* at 944. As the dissent noted, “the Government claims the right to search – without warrant or even a suspicion of criminal activity – any patient’s confidential medical record contained in a computer directory so long as it has a legitimate warrant or subpoena for any other individual patient’s record that may be contained as part of data stored on the same computer.” *Id.* The dissent labeled this theory “novel.”

⁹⁰ *Id.* at 950, 959.

⁹¹ *Id.* at 947.

⁹² *Id.* at 949.

⁹³ *Id.* at 969.

⁹⁴ *Id.* at 973-74.

⁹⁵ *Id.* at 975-76 (arguing that under the majority's plan – which would allow the Government to retain all commingled data – the Fourth Amendment would be rendered a “nullity in the electronic context,” because commingling is an inherent aspect of relational databases).

⁹⁶ *Id.* at 976.

⁹⁷ *See, e.g., United States v. Martinez*, 241 F.3d 1329, 1330-31 (11th Cir. 2001) (citing cases from the Second, Third, Sixth, Seventh, Eighth, and Ninth Circuits agreeing with the court's holding that a district court could exercise equitable jurisdiction over a Rule 41(g) motion after criminal proceedings had concluded).

⁹⁸ *See* FEDERAL PRACTICE AND PROCEDURE §673, at 335.

⁹⁹ *See id.* at 336 (noting that a Rule 41(g) motion is permissible as to an “aggrieved party,” even when the underlying search and/or seizure was lawful), 338 (addressing the suppression of contraband and of items for which the movant has no right of return).

¹⁰⁰ *See* FED. R. CRIM. P. 12(b)(3), (c), (h); *see also United States v. Rollins*, 522 F.2d 160, 166-67 (2d Cir.), *cert. denied*, 424 U.S. 918 (1975).

¹⁰¹ *See* FEDERAL PRACTICE AND PROCEDURE §661, at 37 (stating that the “protection guaranteed by the Fourth Amendment is implemented primarily by the ‘exclusionary rule,’ the rule that evidence that has been illegally seized cannot be admitted in evidence in a criminal trial”); *see also Weeks v. United States*, 232 U.S. 383, 398 (1914) (establishing the exclusionary rule in the federal courts); *Mapp v. Ohio*, 367 U.S. 643, 648-50 (1961) (extending the reach of the exclusionary rule to the states).

¹⁰² As the courts have noted, there are two categories of Rule 41 violations: those that implicate constitutional concerns, and those that do not. *See, e.g., United States v. Simmons*, 206 F.3d 392, 403 (4th Cir. 2000); *United States v. Chaar*, 137 F.3d 359, 362-63 (6th Cir. 1998). Rule 41(h) motions to suppress are concerned solely with constitutional, not technical, violations of Rule 41.

¹⁰³ *See, e.g., United States v. Marx*, 635 F.2d 436, 439 (5th Cir. 1981) (stating the rule).

¹⁰⁴ *See, e.g., Leon*, 468 U.S. at 922 n.23 (noting that the “good faith” inquiry is limited to an objective question, to wit, whether a reasonably well-trained government agent would have

known that the search was illegal, despite the magistrate's authorization); *Riccardi*, 405 F.3d at 861 (applying the "good faith" exception to a search for computer data under a facially invalid warrant); *United States v. Santa*, 180 F.3d 20, 25 (2d Cir. 1999) (holding that the burden is on the Government to demonstrate the objective reasonableness of the searching officer's reliance on an invalid search warrant).

¹⁰⁵ *E.g.*, *Mincey v. Arizona*, 437 U.S. 385, 390-91 (1978) (noting the government's burden to prove an exception to the search warrant requirement); *cf.* *United States v. Johnson*, 495 F.3d 536, 542-44 (7th Cir. 2007) (upholding a search of the defendant's computer equipment and apartment, even in the absence of a warrant or voluntary consent).

¹⁰⁶ *E.g.*, *United States v. Mendenhall*, 446 U.S. 544, 557 (1980) (holding that the Government bears the burden of proving that an individual's consent to search was voluntary).

¹⁰⁷ *See Nardone v. United States*, 308 U.S. 338, 341 (1939) (establishing the "fruit of the poisonous tree" doctrine of evidence suppression).

¹⁰⁸ *See Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920) (holding that evidence is not inadmissible, though obtained as the "fruit" of an illegal search, if the Government learned of the evidence from a source independent of the tainted evidence); *see also Harrison v. United States*, 392 U.S. 219, 225 n.12 (1968) (holding that the burden is on the Government to establish an independent source for the tainted evidence).

¹⁰⁹ *See Nix v. Williams*, 467 U.S. 431, 443 (1984) (holding that exclusion is not proper where the Government can prove, by a preponderance of the evidence, that it would ultimately or inevitably have discovered the challenged information by lawful means); *United States v. Larsen*, 127 F.3d 984, 986 (10th Cir.), *cert. denied*, 522 U.S. 1140 (1997) (holding that the "inevitable discovery" exception applies whenever an independent investigation would ineluctably have uncovered the challenged evidence, even if such an investigation was not ongoing at the time of the illegal police conduct).

¹¹⁰ *See Segura v. United States*, 468 U.S. 796, 799 (1984) (upholding the denial of suppression where the Government discovered the evidence at issue during a lawful, warranted search that was wholly unrelated to an allegedly illegal entry that had occurred the previous day); *see also United States v. Ceccolini*, 435 U.S. 268, 275 (1978) (upholding denial of suppression where the passage of time had attenuated the connection between a police officer's illegal search of an envelope at the defendant's flower store, the officer's contact with a store clerk, and the store clerk's voluntary testimony at trial); *Wong Sun v. United States*, 371 U.S. 471, 491 (1963) (holding that the passage of time between the defendant's illegal arrest and the time that he made incriminating statements to the police "attenuated" any connection between the two and "dissipate[d] the taint" of the illegal arrest).

¹¹¹ *See United States v. Sells*, 463 F.3d 1148, 1155 (10th Cir. 2006) (finding that "every federal court to consider the issue has adopted the doctrine of severance, whereby valid portions of a

warrant are severed from the invalid portions and only materials seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible”); *United States v. George*, 975 F.2d 72, 79 (2d Cir. 1992) (adopting the doctrine of severance); *United States v. Riggs*, 690 F.2d 298, 301 (1st Cir. 1982) (observing that blanket exclusion for a partially-invalid warrant “would seem ill advised”); *United States v. Christine*, 687 F.2d 749, 758 (3d Cir. 1982) (observing that the cost of suppressing all evidence collected under a partially-invalid warrant is too great to justify).

¹¹² We are omitting from this discussion any proposals advanced by “electronic search and seizure pundits” – many of whom are cited elsewhere in this article – largely because their proposed solutions to the “overbreadth” problem require legislative action and/or fundamental changes in existing Fourth Amendment jurisprudence. Both of these topics are not only beyond the scope of this article, they are also generally beyond the ability of the criminal defense practitioner to influence, at least in the short run. Thus, we will focus our discussion on practical, short-term measures.

¹¹³ See 28 CFR §59.1 *et seq.* (2006), and United States Attorneys’ Manual §9-19.00, *et seq.* (2006) (hereinafter “USAM”), respectively.

¹¹⁴ See 28 CFR §§59.1(b), 59.4(a); USAM §§9-19.200, 9-19.210.

¹¹⁵ See 28 CFR §59.4(b)(1); USAM §§9-19.220, 9-19.230 (noting that “there may be additional third-party professionals (e.g., psychologists, psychiatric social workers, or nurses) who possess materials containing private information similar to that held by doctors[, and t]he regulations are intended to cover these relationships as well”).

¹¹⁶ DOJ Manual, *supra* note 28, at 46 (emphasis added). See also *id.* at 47-48 (suggesting that, where possible, agents describe how they intend to search for targeted files among commingled, innocuous documents).

¹¹⁷ *Id.* at 47.

¹¹⁸ See *Comprehensive Drug Testing, Inc.*, 473 F.3d at 939-40 (describing a post-seizure review of potentially irrelevant or privileged materials by a neutral magistrate); see also Amy Baron-Evans and Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 Boston Bar J. 10, at *12-13 (May/June 2003) (discussing methods for screening irrelevant and privileged information from ESI searches prior to use by the Government).

¹¹⁹ See DOJ Manual, *supra* note 28, at 40.

¹²⁰ See *id.*; see also *5444 Westheimer Road*, 2006 U.S. Dist. Lexis 48850, at *8-9 (approving the use of a government taint team to review potentially privileged documents in order to permit expeditious review and the continuation of the Government’s investigation).

¹²¹ See, e.g., *Hunter*, 13 F. Supp. 2d at 583 n.2 (asserting that review by a magistrate judge or special master is preferable to reliance on a taint team); *In re Search of McCorkle*, 972 F. Supp. 1423, 1437 (M.D. Fla. 1997) (disapproving of the use of government taint teams to review privileged materials); *United States v. Neill*, 952 F. Supp. 834, 841 n.14 (D.D.C. 1997) (same); *In re Search Warrant of Law Offices Executed on March 17, 1992*, 153 F.R.D. 55, 57 (S.D.N.Y. 1994) (same).

¹²² See Marcellus McRae, Brian Goebel, and Mark Mermelstein, *What to Do When Your Client's Office is Searched*, 49 No. 5 PRAC. LAW. 23, Oct. 2003, at *31-32 (advising clients that they should not rely on the government to screen the clients' privileged materials).

¹²³ See, e.g., *United States v. Abbell*, 914 F. Supp. 519, 520-21 (S.D. Fla. 1995) (appointing a special master to review seized computer data for privilege).

¹²⁴ See DOJ Manual, *supra* note 28, at 40.

¹²⁵ See DOJ Manual, *supra* note 28, at 40 (citing *United States v. Skeddle*, 989 F. Supp. 890, 893 (N.D. Ohio 1997) (declining to conduct an *in camera* review of seized materials)). *But see Klitzman*, 744 F.2d at 962 (approving the use of a magistrate to conduct the file review).

¹²⁶ See *Comprehensive Drug Testing, Inc.*, 473 F.3d at 939-40 (holding that "upon a proper post-seizure motion by the aggrieved parties, the record should be sealed and reviewed by a magistrate – such as the one who originally issued the warrant").

¹²⁷ The author is not a computer forensic expert and will not endeavor (because he is not qualified) to explain the technical aspects, or limitations, of data encryption. Rather, this section of the article is an exhortation to defense counsel to address these issues with their clients and, if appropriate, to consult with experts to determine feasible proactive steps.

¹²⁸ Wikipedia, The Free Encyclopedia, *Cryptography*, <http://en.wikipedia.org/wiki/cryptography> (last visited January 18, 2007).

¹²⁹ The author is not here advocating the alteration, destruction, concealment, or deletion of data, nor is the author advocating obstruction of justice or the defiance of a lawful grand jury subpoena. Indeed, armed with a valid search warrant, the Government may be able to seize the client's entire computer system and/or to seize all ESI contained therein. Barring any statute or regulation to the contrary, however, the client has no legal obligation to store its data in an "open" format or voluntarily to decrypt data seized by the Government. See A. Michael Froomkin, *The Constitution and Encryption Regulation: Do We Need A "New Privacy?"* 3 LEG. & PUB. POLICY 25, 30 (1999-2000) (noting that the Fourth Amendment does not give the Government a right to an "effective search," nor impose on citizens the obligation to help the Government in its search efforts). Indeed, the Government's prior efforts to ensure unrestricted access to domestic encrypted data never came to fruition. See *United States v. Scarfo*, 180 F.

Supp. 2d 572, 583 n.6 (D. N.J. 2001) (noting that the Cyberspace Electronic Security Act of 1999 – which would have required U.S. citizens to place their encryption keys in an escrow for use by the Government during criminal investigations – “died in Congress before being acted upon”).

¹³⁰ Although “one-time pads” are the only theoretically unbreakable cipher system, the security of other encryption algorithms depends on the amount of effort required to use them, in contrast to the effort required to break them. So-called “brute force attacks” use computational power to discern keys from groups of unencrypted (plaintext) and encrypted (ciphertext) documents, but the effort required to decipher encrypted text in this manner is exponentially dependent on the key size, such that trillions of computations may be required in order to break a given cipher. *Cryptography*, *supra* noted 128.

¹³¹ The Fifth Amendment provides, in pertinent part, that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.” U.S. Const., amend. V. This privilege applies to any statement that might tend to incriminate the witness, even if it merely “furnish[es] a link in the chain of evidence needed to prosecute the claimant for a . . . crime.” *Hoffman v. United States*, 341 U.S. 479, 486-87 (1951). *See also Ohio v. Reiner*, 532 U.S. 17, 18 (2001) (affirming that the Fifth Amendment “protects the innocent as well as the guilty” from possible self-incrimination).

¹³² *See In re Grand Jury Subpoena to Sebastien Boucher*, No. 2:06-mj-91, 2007 WL 4246473, at *3-4 (D. Vt. Nov. 29, 2007). In *Boucher*, the Government “concede[d] that it cannot compel Boucher to disclose the [encryption] password to the grand jury because the disclosure would be testimonial.” *Id.* at *3. Nonetheless, the Government argued that if Boucher merely entered the password, without anyone observing it, there would be no “testimony” and, thus, no Fifth Amendment issue. *Id.* at *3-4. The Court rejected this argument and held that the mere use of the password had “communicative aspects” and could constitute an admission that Boucher knew the evidence existed, was authentic, and was within his control. *Id.* at *3 (citing *Doe v. United States*, 497 U.S. 201, 209 (1988)).

¹³³ *See supra* note 19.

¹³⁴ *See, e.g., Hoffman*, 341 U.S. at 486 (holding that the Fifth Amendment privilege “not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant”).

¹³⁵ *See Braswell v. United States*, 487 U.S. 99, 107-08 (1988) (holding that “collective entities” such as corporations, partnerships, and labor organizations enjoy no privilege against self-incrimination and requiring production of possibly incriminatory records from the president/sole shareholder of the target company); *Bellis v. United States*, 417 U.S. 85, 88 (1974); *Curcio v. United States*, 354 U.S. 118, 122-23 (1957) (finding that a corporate custodian of records must

answer basic questions about the records produced, though not to the point of “condemn[ing] himself by his own oral testimony”); *Hale v. Henkel*, 201 U.S. 43 (1906).

¹³⁶ See *Fischer v. United States*, 425 U.S. 391, 412-13 (1976); see also *In re Grand Jury Proceedings of United States*, 625 F.2d 1051, 1055 (1st Cir. 1980) (noting the Supreme Court’s rejection of Fifth Amendment privileges with respect to business records).

¹³⁷ See FED. R. CRIM. P. 17(c)(2) (2007).

¹³⁸ See *supra* note 94; see also *In re Grand Jury Subpoenas*, 454 F.3d at 524 (allowing intervention by a third party who claimed the attorney-client privilege as to documents held by the subpoenaed party and permitting the third party to review and to withhold from production any privileged documents).

¹³⁹ In theory, the Government could also seek a warrant for the placement of a “key logger system” (“KLS”) on the client’s computer (or computer system), in order to record the keystrokes comprising the password or key. See *Scarfo*, 180 F. Supp. 2d at 574. Not only would the use of a KLS be difficult in the context of a typical business (On whose computer would the Government install the KLS? How would the Government bypass physical and cyber-security?), but a client facing demands for production of the key could take steps to monitor its systems and to detect the use of KLS technology before the Government could obtain the desired information.