The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2012
PHILADELPHIA, WEDNESDAY, AUGUST 22, 2012 VOL 246 • NO. 37 An ALM Publication

WHITE-COLLAR LAW

Protocol for Discovery of Electronic Data in Criminal Cases

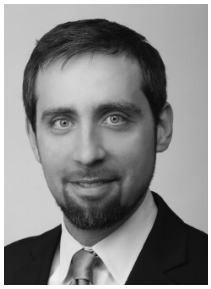
BY PETER D. HARDY AND ABRAHAM REIN
Special to the Legal

Increasingly, criminal lawyers — like their civil counterparts — are faced with legal and practical problems flowing from the potential enormity of the electronically stored information (ESI) involved in discovery. Earlier this year, the Department of Justice and the Federal Defenders attempted to alleviate or at least address some of these problems by issuing a set of recommendations for discovery of ESI in criminal cases. The document, sometimes referred to as "the protocol," is the first of its kind and has the potential to change for the better the way post-indictment discovery is handled in criminal litigation involving high volumes of digital data. Such change, however, will require practitioners to seize the opportunity the protocol represents by becoming familiar with it, treating it seriously as a discovery framework and educating opposing counsel and courts about it.

Although the protocol states that its violation "may not serve as a basis for allegations of misconduct or claims for relief," it currently is the closest thing that the criminal bar has to rules regarding the conduct of electronic discovery, something attorneys and courts alike have been increasingly calling for in recent years. Accordingly, the protocol — or some future version of it — could become a crucial document for criminal practitioners, influencing the contours of all federal criminal litigation, particularly in the document-intensive realm of white-collar offenses.

How much real-world impact the protocol — a nonbinding document that depends upon mutual cooperation by the parties — actually will have remains to be seen. Further, there are many significant issues that the protocol does not address, such as the burden and expense imposed by extremely broad grand jury subpoenas and any obligations of the government under *Brady v. Maryland* to direct the defense to exculpatory evidence buried within voluminous electronic discovery. Nonetheless, the protocol is original and unique to federal criminal practice and therefore merits discussion on that basis alone.


HARDY


REIN

PETER D. HARDY *(phardy@postschell.com)* and **ABRAHAM REIN** *(arein@postchell.com) are attorneys in the Philadelphia office of the law firm of Post & Schell, and are part of the firm's white-collar defense, internal investigations and corporate compliance practice, as well as its data protection group. Hardy previously served as an assistant U.S. attorney and is the author of* Criminal Tax, Money Laundering, and Bank Secrecy Act Litigation. *Rein's experience with managing electronic information includes having co-founded and served as the managing partner of a Web-development and consulting firm.*

CONTENT OF THE PROTOCOL

Although the protocol covers more issues than can be summarized here adequately, some of the key points include:

• Emphasis on the importance of early, collaborative discussions between the parties regarding electronic discovery issues. Such discussions should seek to avoid later disputes and ensure that discovery and litigation proceed smoothly and efficiently. The protocol details a variety of specific topics that should be covered, including the type, format and quantity of ESI to be produced; how best to address privileged or confidential information buried in a production; software or hardware limitations of either party; and how the parties propose to ensure the security of the data.

• Attorneys bear a special responsibility to develop an "adequate understanding" of electronic discovery. When appropriate, attorneys should bring in others who have sufficient knowledge and experience regarding ESI.

• Regarding the often expensive and labor-intensive process of preparing ESI for production — extracting usable data from varied media, converting material from one format to another and the like — the protocol recommends that the producing party not be required "to take on substantial additional processing or format conversion costs and burdens beyond what that party has already done or would do for its own case preparation or discovery production." There is, however, an important corollary to that rule: To the extent a producing party takes on the burden and expense of processing the data for its own case, the results of that processing should be produced to the other side, barring compelling countervailing considerations. This principle likely will be a source of friction, as resource-scarce defendants may contest whether the government has processed data sufficiently to meet its discovery obligations under *Brady* and Federal Rule of Criminal Procedure 16, even if the government has prepared its own case to its own satisfaction.

CASE STUDY: *UNITED STATES V. STIRLING*

Whether the protocol will have practical impact, or instead will be relegated to representing only ideals embraced in theory but ignored in practice, remains to be seen. A recent decision in *United States v. Stirling*, 1:11-cr-20792-CMA, slip op. (S.D. Fla. June 5, 2012), provides an illustration of how the protocol might change litigation in practice, and how the parties and court would have benefited from its application.

In *Stirling*, according to court opinions, the defendant, John Philip Stirling, was apprehended on his boat, which was carrying a large amount of illegal drugs. He and his shipmates were arrested and charged with conspiracy and possession with intent to distribute the drugs. Stirling's co-defendants pled guilty; Stirling maintained a duress defense.

Stirling's laptop was seized from the boat and the government produced to the defense an "exact replica" of the computer's hard drive. Stirling's lawyer reviewed that electronic production by accessing the drive and clicking through the documents she saw there, opening folders and documents one by one.

According to court filings, this review yielded some material that the attorney viewed as potentially damaging to her client, including a photograph of him with a large amount of currency. During a conference with counsel for the government, she was told that if the defendant took the stand and testified falsely, the government would use evidence from the computer during its rebuttal case. The client nonetheless testified at trial, alleging that he and his family had been threatened by Colombian drug traffickers and that his alleged participation in the crime resulted from duress.

During its rebuttal case, the government called an FBI computer analyst who — unbeknownst to the defense — had performed a forensic examination on the laptop and had recovered, with the help of specialized software, voluminous deleted logs of Stirling's instant message exchanges. Stirling's lawyer had been unaware of these transcripts when she framed her case and advised her client regarding testifying. According to the district court, the messages had a "devastating impact" on his duress defense, contradicted many of the statements made during the defendant's testimony, and "irreparably" damaged his credibility. The jury found him guilty on all counts.

MOTION FOR A NEW TRIAL

Stirling moved for a new trial, arguing that the government had not complied with its obligations under Federal Rule of Criminal Procedure 16(a)(1)(B)(i) to produce relevant statements made by the defendant. The government responded that it had produced the statements — indeed, it argued, the government had produced an exact replica of Stirling's computer, which contained, bit-for-bit, everything the government had access to, including the instant messaging logs:

"Defendant in essence argues that in order for the government to comply with Rule 16, it is insufficient for the government to produce electronic evidence containing defendant's statements, but that the government has to sift through the electronic evidence, categorize it as Rule 16(a)(1)(B) evidence, print it and provide defendant with the printout."

The defense responded that the "production of something in a manner which is unintelligible is really not production," likening the government's position to "granting access to documents located in a warehouse but not advising the defense that there is a secret basement where the defendant's statements are located." The district court sided with the defense and granted a new trial.

STIRLING UNDER THE PROTOCOL

The protocol had not yet been published when the *Stirling* case was tried for the first time. But *Stirling* provides an informative case study of the protocol's potential for altering criminal litigation. Under the protocol — if actually followed — the case likely would have played out differently.

First, the protocol requires that the parties initiate an effective meet and confer process early on in the litigation. In *Stirling*, the lawyers apparently spoke superficially about the data on the laptop — the government informed defense counsel that the laptop contained potential rebuttal evidence — but there was no further discussion as to the nature, format, volume, etc. of the data at issue.

The protocol is original and unique to federal criminal practice and therefore merits discussion on that basis alone.

The protocol, by contrast, specifically recommends that the meet and confer address issues related to the "inspection of hard drives and/or forensic (mirror) images." It explains:

"Any forensic examination of a hard drive, whether it is an examination of the hard drive itself or an examination of a forensic image of a hard drive, requires specialized software and expertise. A simple copy of the forensic image may not be sufficient to access the information stored, as specialized software may be needed. The parties should consider how to manage inspection of a hard drive and/or production of a forensic image of a hard drive and what software and expertise will be needed to access the information."

If, as the protocol requires, the parties had discussed "what software and expertise will be needed to access the information [on the hard drive]" at an early meet and confer, the fact of the hidden instant message logs may have surfaced pretrial and the new trial order might have been avoided. Of course, the protocol only works if the parties in fact engage in good-faith discussions with sufficient detail. If, for example, a party wants to not highlight the existence of potentially damaging evidence in order to lay a trap, then a discussion conducted so as to preserve that goal will accomplish little. Moreover, even if the protocol had been followed, many lawyers may lack the technical sophistication to know what questions to ask, or how to answer them, as to the forensic investigation of the laptop. Thus, the protocol stresses the need to involve nonlawyers with technical knowledge when necessary.

Even absent an effective meet and confer process, a faithful application of the protocol should have resulted in government production of the restored instant message transcripts. The protocol provides that a party who has undertaken "processing" of ESI for its own use is expected to produce the processed data to the other side, to the extent possible without revealing attorney work product. Accordingly, when the forensic analyst processed the laptop in *Stirling*, the government should have produced the results of that processing — i.e., any deleted data he was able to restore — and the defense would have been aware of it. Conceivably, there might have been no trial at all.

A PROTOCOL WORTH UNDERSTANDING

The *Stirling* case provides a window into the protocol's potential to change the course of a criminal litigation. Criminal law practitioners should become familiar with the protocol — despite, or perhaps because of, the fact that many practitioners are not conversant or comfortable with technology. Although the protocol's impact remains to be seen, practitioners and courts now can help shape its impact, and whether the protocol will turn out to be the start of further reforms, by treating it seriously. •