

New York Law Journal

Technology Today

WWW.NYLJ.COM

An ALM Publication

©2009 INCISIVE MEDIA US PROPERTIES, LLC

TUESDAY, DECEMBER 8, 2009

ELECTRONIC COMMUNICATION

Bear Stearns Case Highlights Issue of Warrants for E-Mails

By
James M.
Keneally



The recent acquittals of former Bear Stearns hedge fund managers Ralph Cioffi and Matthew Tannin following a jury trial in the Eastern District of New York have received substantial media coverage, as their case was widely considered to be the first prosecution of Wall Street executives following the subprime mortgage crisis and the ensuing financial meltdown.¹ This is understandable, given the attention the economic crisis has received, and the infamy attached to the Bear Stearns meltdown itself.

However, an Oct. 26 opinion in the case by Judge Frederick Block, while not gaining the notoriety the trial verdict did, might be at least as significant for those practitioners dealing with the vexing issues surrounding the search and seizure of computer files. Judge Block's opinion serves as a useful and comprehensive guide to the current state of the law, and of issues with which we can expect to wrestle in the near future.

Here are the facts. Cioffi and Tannin managed two hedge funds for Bear Stearns Asset Management (BSAM). The funds collapsed in 2007, and the Securities and Exchange Commission and the Eastern District U.S. Attorney's Office launched investigations into the collapse. In November 2007, BSAM turned over to the SEC and the U.S. attorney an April 22, 2007, e-mail that Tannin had sent to Cioffi from his personal Google Gmail account. As recounted in the indictment against Cioffi and Tannin, the e-mail read, in part, "[T]he subprime market looks pretty damn ugly. ... If we believe the [CDO report is] ANYWHERE close to accurate I think we should close the funds now. The reason for this is that if [the CDO report] is correct the entire subprime market



STOCK: NYLJ

is toast. ...If AAA bonds are systematically downgraded then there is simply no way for us to make money—ever."²

Cioffi and Tannin were indicted in June 2008 and charged with conspiracy, securities fraud and wire fraud related to the funds' demise. The crux of the government's case was that Cioffi and Tannin had touted the funds' health to investors to get them to invest more money in the funds, when in fact they knew the subprime market, and in turn the funds, were teetering on the brink of disaster.

An Oct. 26 opinion by Eastern District Judge Frederick Block offers insight to practitioners dealing with the vexing issues surrounding the search and seizure of computer files.

In February 2009, the government applied to Magistrate Judge Cheryl Pollak for a warrant to search Tannin's e-mail account. The government's application was made pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701-2712.³ The affidavit of FBI Special Agent Mark Munster incorporated the indictment by reference and specifically alluded to the paragraph in the indictment that quoted Tannin's April 22, 2007, e-mail to Cioffi as evidence that Tannin had used his Gmail account to further the alleged conspiracy.

Agent Munster's affidavit further set forth the procedures that would be followed during the search. He stated that only e-mails created prior to Aug. 12, 2007, when Tannin retained counsel, would be searched.

He further stated that the measures that needed to be taken in searching electronic files "would be impractical to do at Google's offices" and needed to be done off-site and "in a controlled environment," and that law enforcement officers would "segregate any messages and content constituting evidence of violations of federal criminal law."

Finally, Agent Munster's affidavit asserted that Tannin's Gmail account contained evidence of conspiracy, securities fraud and wire fraud.

Magistrate Judge Pollak signed the warrant. It authorized the search of the "premises known and described as 'matt.tannin@gmail.com,'" and the seizing of the items set forth in an addendum, "Schedule A," to the warrant. "Schedule A" listed, among other items, "all e-mail up through August 12, 2007, including any attachments, and all instant messages, sent by or received by the accounts [sic], whether saved or deleted, whether contained directly in the e-mail account or in a customized folder." There was no other language in the warrant or Attachment A limiting the scope of the items to be seized, nor was Agent Munster's affidavit attached to the warrant.

As will be discussed, the failure to attach the affidavit to the warrant ultimately proved to be the warrant's undoing.

Initially Google informed the government that Tannin's account had been deleted and the requested files could no longer be extracted. Then, on the eve of trial, Google informed the government that it had found a copy of Tannin's file as it existed on Nov. 6, 2007.

Google provided the government with a CD-ROM containing a copy of the account as it existed on that date. During a search of the account, the government found a Nov. 23, 2006, e-mail from Tannin to himself. It contained, among other things, Tannin's personal thoughts

JAMES M. KENEALLY, a partner at Kelley Drye & Warren, focuses on the defense of clients in white-collar crime and investigation matters. NAFEEES NURUDDIN, a litigation associate at the firm, assisted in the preparation of this article.

(or, as Judge Block described them, “anxiety”) about his job and the state of the market.

The government sought to introduce Tannin’s e-mail as evidence of his knowledge and intent concerning the crimes with which he was charged. Tannin moved to suppress the e-mail, arguing that the warrant was invalid on its face because it failed to describe with particularity the items to be seized, and that it was impermissibly overbroad.

Warrants Clause

Judge Block granted Tannin’s motion and suppressed the e-mail. The judge began with the proposition that the “overarching purpose” of the Fourth Amendment’s warrants clause “is to ensure that ‘those searches deemed necessary should be as limited as possible.’”⁴

The warrants clause achieves this, Judge Block wrote, by requiring particularity and forbidding overbreadth. Quoting his own recent opinion in *United States v. Cohan*, Judge Block explained that “a warrant can violate the clause ‘either by seeking specific material as to which no probable cause exists, or by so vague a description of the material sought as to impose no meaningful boundaries.’”⁵

He then acknowledged that the degree of particularity required in a warrant depends in part on the type of evidence being sought. In this regard, he stated, “courts have recognized that documentary evidence may be difficult to describe ex ante with the same particularity as a murder weapon or stolen property.”⁶

At the same time, Judge Block noted, our courts have expressed concern over the “grave dangers inherent in executing a warrant authorizing a search and seizure of a person’s papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable.”⁷ And, he went on, “[t]he dawn of the Information Age has only heightened those concerns.”⁸

Judge Block explained that computer-based documents are a double-edged sword when it comes to privacy issues. Quoting Judge Kenneth M. Karas of the Southern District of New York in *United States v. Vilar*, he pointed out that on one hand, computers “often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize,” while on the other hand, “it is precisely because computer files can be intermingled and encrypted that the computer is a useful criminal tool.”⁹

In applying the current law to the facts, Judge Block relied chiefly on *Groh v. Ramirez*.¹⁰ *Groh* was a *Bivens* action involving an ATF search pursuant to warrant of a ranch for weapons believed to be on the premises. The affidavit in support of the warrant detailed the weapons the agent believed to be on the premises. However, the warrant itself did not describe any of the sought-after weapons. It described only the house to be searched. The affidavit was not attached to the warrant, having been sealed, nor did the warrant incorporate it by reference.

The U.S. Supreme Court, with Justice John Paul Stevens writing for the majority, held, as the defendant ATF agent conceded, that the warrant itself was invalid because it failed to describe the items sought to be seized.

The Court further held that the warrant could not be saved from its invalidity from the fact that the application in support of its issuance adequately described those items: “The fact that the *application* adequately described the ‘things to be seized’ does not save the *warrant* from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting document.”¹¹

The Court in *Groh* recognized that numerous circuit courts had held that a warrant was sufficiently particular in its description of the items sought if it incorporated the supporting affidavit by reference, and if the affidavit was attached to the warrant. However, because the warrant in *Groh* neither incorporated nor attached the supporting affidavit, Justice Stevens wrote, “we need not further explore the matter of incorporation.”¹²

In his decision, Judge Block noted that prior to *Groh*, the U.S. Court of Appeals for the Second Circuit, in *United States v. Bianco*,¹³ had eschewed the formal requirement of incorporation and attachment of the supporting affidavit to an otherwise deficient warrant, in favor of an approach that examined the circumstances of the search itself to determine whether the agents conducting the search were sufficiently advised of the search’s limitations.

However, Judge Block continued, in light of *Groh*, he, previously in *United States v. Cohan*, as well as two other district court judges,¹⁴ had determined that *Bianco* was no longer the law in the Second Circuit.

Judge Block concluded that the warrant seeking Tannin’s e-mails was unconstitutionally broad. He further rejected the government’s arguments urging the applicability of both the “good faith” exception under *United States v. Leon*¹⁵ and the “inevitable discovery” exception provided by *Nix v. Williams*.¹⁶

Ninth Circuit Guidance

Judge Block’s decision in *Cioffi* ultimately hinged on a rather straightforward reading of *Groh*’s technical requirements. However, it also left unanswered for another day issues especially applicable to electronic searches.

For example, the Ninth Circuit has provided the following guidance for magistrate judges to use when considering warrant applications for electronic records:

1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases [internal citation omitted].
2. Segregation and redaction must be either done by specialized personnel or an independent third party [internal citation omitted]...
3. Warrants and subpoenas must disclose the actual risks of destruction

of information as well as prior efforts to seize that information in other judicial fora [internal citation omitted].

4. The government’s search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents [internal citation omitted].

5. The government must destroy, or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept [internal citation omitted].¹⁷

It is questionable, if not doubtful, whether the Second Circuit would adopt such guidance.¹⁸ However, Judge Block’s decision in *Cioffi*, while not specifically deciding these issues, provides practitioners with an interesting and useful jumping-off point for such analysis.

.....●●.....

1. See, e.g., Amir Efrati and Peter Lattman, U.S. loses fraud case tied to Bear Stearns, Wall Street Journal, Nov. 12, 2009; William D. Cohan, How the Scapegoats Escaped, N.Y. Times, Nov. 12, 2009.

2. *United States v. Cioffi*, No. 08-CR-415 (FB), Memorandum and Order at 2, (E.D.N.Y. Oct. 26, 2009), available at <http://www.eff.org/files/US%20v.%20Cioffi.pdf>

3. Specifically, 18 U.S.C. §2703 sets forth the procedure by which the government may obtain communications such as e-mails from providers of communications services. Where the government seeks communications which have been stored in a service provider’s electronic storage system for more than 180 days, and wishes to avoid providing otherwise required notice of that request to the subscriber, it may do so only by the issuance of a search warrant. 18 U.S.C. § 2703 (2006) subsecs. (a), (b) (A).

4. *Cioffi*, No. 08-CR-415 (FB) at 7, quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

5. Op. at 7, quoting *United States v. Cohan*, 628 F.Supp.2d 355, 359 (E.D.N.Y. 2009).

6. Op. at 8.

7. Op. at 9, quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).

8. Op. at 9.

9. Op. at 9, quoting *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at *35 (S.D.N.Y. April 4, 2007).

10. 540 U.S. 551 (2004).

11. 540 U.S. at 557 (emphasis in original).

12. 540 U.S. at 558.

13. 998 F.2d 1112 (2d Cir. 1993).

14. *United States v. Ryan*, No. 2:07-cr-35, 2008 WL 901538, at *2 (D.Vt. Mar. 31, 2008); *Vilar*, 2007 WL 1075041 at *22 n.13.

15. 468 U.S. 897 (1984).

16. 467 U.S. 431 (1984).

17. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2008).

18. See, e.g., *Vilar*, 2007 WL 1075041 at *38 (“a rule that does not require a computer search protocol avoids the courts getting into the business of telling investigators how to conduct a lawful investigation, something the courts are ill-equipped to do.”)