Email this Document!
U.S. Department of Justice
Executive Office for United States Attorneys
United States Attorneys' USA Bulletin
March 2001 Vol. 49, No.2

Computer Records and the Federal Rules of Evidence

Orin S. Kerr

USA Bulletin

(March 2001)

Orin S. Kerr
Trial Attorney
Computer Crime and Intellectual Property Section

This article explains some of the important issues that can arise when the government seeks the admission of computer records under the Federal Rules of Evidence. It is an excerpt of a larger DOJ manual entitled "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", which is available on the internet at www.cybercrime.gov/searchmanual.htm.

Most federal courts that have evaluated the admissibility of computer records have focused on computer records as potential hearsay. The courts generally have admitted computer records upon a showing that the records fall within the business records exception, Fed. R. Evid. 803(6):

Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

See, e.g., United States v. Cestnik, 36 F.3d 904, 909-10 (10th Cir. 1994); *United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990); *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988); *Capital Marine Supply v. M/V Roland Thomas II*, 719 F.2d 104, 106 (5th Cir. 1983). Applying this test, the courts have indicated that computer records generally can be admitted as business records if they were kept

pursuant to a routine procedure for motives that tend to assure their accuracy.

However, the federal courts are likely to move away from this "one size fits all" approach as they become more comfortable and familiar with computer records. Like paper records, computer records are not monolithic: the evidentiary issues raised by their admission should depend on what kind of computer records a proponent seeks to have admitted. For example, computer records that contain text often can be divided into two categories: computer-generated records, and records that are merely computer-stored. *See People v. Holowko*, 486 N.E.2d 877, 878-79 (Ill. 1985). The difference hinges upon whether a person or a machine created the records' contents. Computer-stored records refer to documents that contain the writings of some person or persons and happen to be in electronic form. E-mail messages, word processing files, and Internet chat room messages provide common examples. As with any other testimony or documentary evidence containing human statements, computer-stored records must comply with the hearsay rule. If the records are admitted to prove the truth of the matter they assert, the offeror of the records must show circumstances indicating that the human statements contained in the record are reliable and trustworthy, *see* Advisory Committee Notes to Proposed Rule 801 (1972), and the records must be authentic.

In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records, and ATM receipts tend to be computer-generated records. Unlike computer-stored records, computer-generated records do not contain human "statements," but only the output of a computer program designed to process input following a defined algorithm. Of course, a computer program can direct a computer to generate a record that mimics a human statement: an e-mail program can announce "You've got mail!" when mail arrives in an inbox, and an ATM receipt can state that $100 was deposited in an account at 2:25 pm. However, the fact that a computer, rather than a human being, has created the record alters the evidentiary issues that the computer-generated records present. *See, e.g.*, 2 J. Strong, *McCormick on Evidence* §294, at 286 (4th ed. 1992). The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity). *See id.*; Richard O. Lempert & Steven A. *Saltzburg, A Modern Approach to Evidence* 370 (2d ed. 1983); *Holowko*, 486 N.E.2d at 878-79.

Finally, a third category of computer records exists: some computer records are both computer-generated *and* computer-stored. For example, a suspect in a fraud case might use a spreadsheet program to process financial figures relating to the fraudulent scheme. A computer record containing the output of the program would derive from both human statements (the suspect's input to the spreadsheet program) and computer processing (the mathematical operations of the spreadsheet program). Accordingly, the record combines the evidentiary concerns raised by computer-stored and computer-generated records. The party seeking the admission of the record should address both the hearsay issues implicated by the original input and the authenticity issues raised by the computer processing.

As the federal courts develop a more nuanced appreciation of the distinctions to be made between different kinds of computer records, they are likely to see that the admission of computer records generally raises two distinct issues. First, the government must establish the

authenticity of all computer records by providing "evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). Second, if the computer records are computer-stored records that contain human statements, the government must show that those human statements are not inadmissible hearsay.

A. Authentication

Before a party may move for admission of a computer record or any other evidence, the proponent must show that it is authentic. That is, the government must offer evidence "sufficient to support a finding that the [computer record or other evidence] in question is what its proponent claims." Fed. R. Evid. 901(a). *See United States v. Simpson*, 152 F.3d 1241, 1250 (10th Cir. 1998).

The standard for authenticating computer records is the same as for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. *See United States v. DeGeorgia*, 420 F.2d 889, 893 n.11 (9th Cir. 1969); *United States v. Vela*, 673 F.2d 86, 90 (5th Cir. 1982). *But see United States v. Scholle*, 553 F.2d 1109, 1125 (8th Cir. 1977) (stating in dicta that "the complex nature of computer storage calls for a more comprehensive foundation"). For example, witnesses who testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. *See UnitedStates v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) (citing cases). Instead, the witness simply must have first-hand knowledge of the relevant facts to which he or she testifies. *See generally United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (FBI agent who was present when the defendant's computer was seized can authenticate seized files) *United States v. Miller*, 771 F.2d 1219, 1237 (9th Cir. 1985) (telephone company billing supervisor can authenticate phone company records); *Moore*, 923 F.2d at 915 (head of bank's consumer loan department can authenticate computerized loan data).

Challenges to the authenticity of computer records often take one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created. Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author.

1. Authenticity and the Alteration of Computer Records

Computer records can be altered easily, and opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. For example, in *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997), the government retrieved computer files from the computer of a narcotics dealer named Frost. The files from Frost's computer included detailed records of narcotics sales by three aliases: "Me" (Frost himself, presumably), "Gator" (the nickname of Frost's co-defendant Whitaker), and "Cruz" (the nickname of another dealer). After the government permitted Frost to help retrieve the evidence from his computer and declined to establish a formal chain of custody for the computer at trial, Whitaker argued that the files implicating him through his alias were not properly authenticated.

Whitaker argued that "with a few rapid keystrokes, Frost could have easily added Whitaker's alias, 'Gator' to the printouts in order to finger Whitaker and to appear more helpful to the government." *Id.* at 602.

The courts have responded with considerable skepticism to such unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. *See Whitaker*, 127 F.3d at 602 (declining to disturb trial judge's ruling that computer records were admissible because allegation of tampering was "almost wild-eyed speculation . . . [without] evidence to support such a scenario"); *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."); *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible."). *Id.* at 559. This is consistent with the rule used to establish the authenticity of other evidence such as narcotics. *See United States v. Allen*, 106 F.3d 695, 700 (6th Cir. 1997) ("Merely raising the possibility of tampering is insufficient to render evidence inadmissible."). Absent specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility. *See Bonallo*, 858 F.2d at 1436.

2. Establishing the Reliability of Computer Programs

The authenticity of computer-generated records sometimes implicates the reliability of the computer programs that create the records. For example, a computer-generated record might not be authentic if the program that creates the record contains serious programming errors. If the program's output is inaccurate, the record may not be "what its proponent claims" according to Fed. R. Evid. 901.

Defendants in criminal trials often attempt to challenge the authenticity of computer-generated records by challenging the reliability of the programs. *See, e.g., United States v. Dioguardi*, 428 F.2d 1033, 1038 (2d Cir. 1970); *United States v. Liebert*, 519 F.2d 542, 547-48 (3d Cir. 1975). The courts have indicated that the government can overcome this challenge so long as "the government provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof[.]" *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990). *See also Liebert*, 519 F.2d at 547; *DeGeorgia*, 420 F.2d. at 893 n.11. *Compare* Fed. R. Evid. 901(b)(9) (indicating that matters created according to a process or system can be authenticated with "[e]vidence describing a process or system used . . . and showing that the process or system produces an accurate result"). In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business. *See, e.g., United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) ("[T]he ordinary business circumstances described suggest trustworthiness, .. . at least where absolutely nothing in the record in any way implies the lack thereof.") (computerized tax records held by the IRS); *Briscoe*, 896 F.2d at 1494 (computerized telephone records held by Illinois Bell). When the

computer program is not used on a regular basis and the government cannot establish reliability based on reliance in the ordinary course of business, the government may need to disclose "what operations the computer had been instructed to perform [as well as] the precise instruction that had been given" if the opposing party requests. *Dioguardi*, 428 F.2d at 1038. Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records "resulting from . . . the operation of the computer program" affect only the weight of the evidence, not its admissibility. *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988).

Prosecutors may note the conceptual overlap between establishing the authenticity of a computer-generated record and establishing the trustworthiness of a computer record for the business record exception to the hearsay rule. In fact, federal courts that evaluate the authenticity of computer-generated records often assume that the records contain hearsay, and then apply the business records exception. *See, e.g., UnitedStates v. Linn*, 880 F.2d 209, 216 (9th Cir. 1989) (applying business records exception to telephone records generated "automatically" by a computer); *United States v. Vela*, 673 F.2d 86, 89-90 (5th Cir. 1982) (same). As discussed later in this article, this analysis is technically incorrect in many cases: computer records generated entirely by computers cannot contain hearsay and cannot qualify for the business records exception because they do not contain human "statements." *See* Part B, *infra*. As a practical matter, however, prosecutors who lay a foundation to establish a computer-generated record as a business record will also lay the foundation to establish the record's authenticity. Evidence that a computer program is sufficiently trustworthy so that its results qualify as business records according to Fed. R. Evid. 803(6) also establishes the authenticity of the record. *Compare United States v. Saputski*, 496 F.2d 140, 142 (9th Cir. 1974).

3. Identifying the Author of Computer-Stored Records

Although handwritten records may be penned in a distinctive handwriting style, computer-stored records consist of a long string of zeros and ones that do not necessarily identify their author. This is a particular problem with Internet communications, which offer their authors an unusual degree of anonymity. For example, Internet technologies permit users to send effectively anonymous e-mails, and Internet Relay Chat channels permit users to communicate without disclosing their real names. When prosecutors seek the admission of such computer-stored records against a defendant, the defendant may challenge the authenticity of the record by challenging the identity of its author.

Circumstantial evidence generally provides the key to establishing the authorship and authenticity of a computer record. For example, in *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998), prosecutors sought to show that the defendant had conversed with an undercover FBI agent in an Internet chat room devoted to child pornography. The government offered a printout of an Internet chat conversation between the agent and an individual identified as "Stavron," and sought to show that "Stavron" was the defendant. The district court admitted the printout in evidence at trial. On appeal following his conviction, Simpson argued that "because the government could not identify that the statements attributed to [him] were in his handwriting, his writing style, or his voice," the printout had not been authenticated and should have been excluded. *Id.* at 1249.

The Tenth Circuit rejected this argument, noting the considerable circumstantial evidence that "Stavron" was the defendant. *See id.* at 1250. For example, "Stavron" had told the undercover agent that his real name was "B. Simpson," gave a home address that matched Simpson's, and appeared to be accessing the Internet from an account registered to Simpson. Further, the police found records in Simpson's home that listed the name, address, and phone number that the undercover agent had sent to "Stavron." Accordingly, the government had provided evidence sufficient to support a finding that the defendant was "Stavron," and the printout was properly authenticated. *See id.* at 1250. *See also United States v. Tank*, 200 F.3d 627, 630-31 (9th Cir. 2000) (concluding that district court properly admitted chat room log printouts in circumstances similar to those in *Simpson*). *But see United States v. Jackson*, 208 F.3d 638 (7th Cir. 2000) (concluding that web postings purporting to be statements made by white supremacist groups were properly excluded on authentication grounds absent evidence that the postings were actually posted by the groups).

B. Hearsay

Federal courts have often assumed that all computer records contain hearsay. A more nuanced view suggests that in fact only a portion of computer records contain hearsay. When a computer record contains the assertions of a person, whether or not processed by a computer, the record can contain hearsay. In such cases, the government must fit the record within a hearsay exception such as the business records exception, Fed. R. Evid. 803(6). When a computer record contains only computer-generated data untouched by human hands, however, the record cannot contain hearsay. In such cases, the government must establish the authenticity of the record, but does not need to establish that a hearsay exception applies for the records to be admissible.

1. Inapplicability of the Hearsay Rules to Computer-Generated Records

The hearsay rules exist to prevent unreliable out-of-court statements by human declarants from improperly influencing the outcomes of trials. Because people can misinterpret or misrepresent their experiences, the hearsay rules express a strong preference for testing human assertions in court, where the declarant can be placed on the stand and subjected to cross-examination. *See Ohio v. Roberts*, 448 U.S. 56, 62-66 (1980). This rationale does not apply when an animal or a machine makes an assertion: beeping machines and barking dogs cannot be called to the witness stand for cross-examination at trial. The Federal Rules have adopted this logic. By definition, an assertion cannot contain hearsay if it was not made by a human being. Can we just use the word person? *See* Fed. R. Evid. 801(a) ("A 'statement' is (1) an oral or written assertion or (2) nonverbal conduct *of a person*, if it is intended by the person as an assertion.") (emphasis added) ; Fed. R. Evid. 801(b) ("A declarant is *a person* who makes a statement.") (emphasis added).

As several courts and commentators have noted, this limitation on the hearsay rules necessarily means that computer-generated records untouched by human hands cannot contain hearsay. One state supreme court articulated the distinction in an early case involving the use of automated telephone records:

The printout of the results of the computer's internal operations is not hearsay evidence. It does not represent the output of statements placed into the computer by out of court declarants. Nor can we say that this printout itself is a "statement" constituting hearsay evidence. The underlying rationale of the hearsay rule is that such statements are made without an oath and their truth cannot be tested by cross-examination. Of concern is the possibility that a witness may consciously or unconsciously misrepresent what the declarant told him or that the declarant may consciously or unconsciously misrepresent a fact or occurrence. With a machine, however, there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly.

State v. Armstead, 432 So.2d 837, 840 (La. 1983). *See also People v. Holowko*, 486 N.E.2d 877, 878-79 (Ill. 1985) (automated trap and trace records); *United States v. Duncan*, 30 M.J. 1284, 1287-89 (N-M.C.M.R. 1990) (computerized records of ATM transactions); 2 J. Strong, *McCormick on Evidence* §294, at 286 (4th ed.1992); Richard O. Lempert & Stephen A. Saltzburg, *A Modern Approach to Evidence* 370 (2d ed. 1983). *Cf. United States v. Fernandez-Roque*, 703 F.2d 808, 812 n.2 (5th Cir. 1983) (rejecting hearsay objection to admission of automated telephone records because "the fact that these calls occurred is not a hearsay statement."). Accordingly, a properly authenticated computer-generated record is admissible. *See* Lempert & Saltzburg, at 370.

The insight that computer-generated records cannot contain hearsay is important because courts that assume the existence of hearsay may wrongfully exclude computer-generated evidence if a hearsay exception does not apply. For example, in *United States v. Blackburn*, 992 F.2d 666 (7th Cir. 1993), a bank robber left his eyeglasses behind in an abandoned stolen car. The prosecution's evidence against the defendant included a computer printout from a machine that tests the curvature of eyeglass lenses. The printout revealed that the prescription of the eyeglasses found in the stolen car exactly matched the defendant's. At trial, the district court assumed that the computer printout was hearsay, but concluded that the printout was an admissible business record according to Fed. R. Evid. 803(6). On appeal following conviction, the Seventh Circuit also assumed that the printout contained hearsay, but agreed with the defendant that the printout could not be admitted as a business record:

the [computer-generated] report in this case was not kept in the course of a regularly conducted business activity, but rather was specially prepared at the behest of the FBI and with the knowledge that any information it supplied would be used in an ongoing criminal investigation. . . . In finding this report inadmissible under Rule 803(6), we adhere to the well-established rule that documents made in anticipation of litigation are inadmissible under the business records exception.

Id. at 670. See also Fed. R. Evid. 803(6) (stating that business records must be "made . . . by, or transmitted by, a person").

Fortunately, the *Blackburn* court ultimately affirmed the conviction, concluding that the computer printout was sufficiently reliable that it could have been admitted under the residual hearsay exception, Rule 803(24). *See id.* at 672. However, instead of flirting with the idea of excluding the printouts because Rule 803(6) did not apply, the court should have asked whether

the computer printout from the lens-testing machine contained hearsay at all. This question would have revealed that the computer-generated printout could not be excluded on hearsay grounds because it contained no human "statements."

2. Applicability of the Hearsay Rules to Computer-Stored Records

Computer-stored records that contain human statements must satisfy an exception to the hearsay rule if they are offered for the truth of the matter asserted. Before a court will admit the records, the court must establish that the statements contained in the record were made in circumstances that tend to ensure their trustworthiness. *See, e.g., Jackson*, 208 F.3d at 637 (concluding that postings from the websites of white supremacist groups contained hearsay, and rejecting the argument that the postings were the business records of the ISPs that hosted the sites).

As discussed earlier in this article, courts generally permit computer-stored records to be admitted as business records according to Fed. R. Evid. 803(6). Different circuits have articulated slightly different standards for the admissibility of computer-stored business records. Some courts simply apply the direct language of Fed. R. Evid. 803(6). *See e.g.,United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991); *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988). Other circuits have articulated doctrinal tests specifically for computer records that largely (but not exactly) track the requirements of Rule 803(6). *See, e.g., United States v. Cestnik*, 36 F.3d 904, 909-10 (10th Cir. 1994) ("Computer business records are admissible if (1) they are kept pursuant to a routine procedure designed to assure their accuracy; (2) they are created for motives that tend to assure accuracy (e.g., not including those prepared for litigation); and (3) they are not themselves mere accumulations of hearsay.") (quoting *Capital Marine Supply v. M/V Roland Thomas II*, 719 F.2d 104, 106 (5th Cir. 1983)); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990) (computer-stored records are admissible business records if they "are kept in the course of regularly conducted business activity, and [that it] was the regular practice of that business activity to make records, as shown by the testimony of the custodian or other qualified witness.") (quoting *United States v. Chappell*, 698 F.2d 308, 311 (7th Cir. 1983)). Notably, the printout itself may be produced in anticipation of litigation without running afoul of the business records exception. The requirement that the record be kept "in the course of a regularly conducted business activity" refers to the underlying data, not the actual printout of that data. *See United States v. Sanders*, 749 F.2d 195, 198 (5th Cir. 1984).

From a practical perspective, the procedure for admitting a computer-stored record pursuant to the business records exception is the same as admitting any other business record. Consider an e-mail harassment case. To help establish that the defendant was the sender of the harassing messages, the prosecution may seek the introduction of records from the sender's ISP showing that the defendant was the registered owner of the account from which the e-mails were sent. Ordinarily, this will require testimony from an employee of the ISP ("the custodian or other qualified witness") that the ISP regularly maintains customer account records for billing and other purposes, and that the records to be offered for admission are such records that were made at or near the time of the events they describe in the regular course of the ISP's business. Again, the key is establishing that the computer system from which the record was obtained is maintained in the ordinary course of business, and that it is a regular practice of the business to rely upon those records for their accuracy.

The business record exception is the most common hearsay exception applied to computer records. Of course, other hearsay exceptions may be applicable in appropriate cases. *See, e.g., Hughes v. United States*, 953 F.2d 531, 540 (9th Cir. 1992) (concluding that computerized IRS forms are admissible as public records under Fed. R. Evid. 803(8)).

C. Other Issues

The authentication requirement and the hearsay rule usually provide the most significant hurdles that prosecutors will encounter when seeking the admission of computer records. However, some agents and prosecutors have occasionally considered two additional issues: the application of the best evidence rule to computer records, and whether computer printouts are "summaries" that must comply with Fed. R. Evid. 1006.

1. The Best Evidence Rule

The best evidence rule states that to prove the content of a writing, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required. See Fed. R. Evid. 1002. Agents and prosecutors occasionally express concern that a mere printout of a computer-stored electronic file may not be an "original" for the purpose of the best evidence rule. After all, the original file is merely a collection of 0's and 1's. In contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes.

Fortunately, the Federal Rules of Evidence have expressly addressed this concern. The Federal Rules state that

[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".

Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule. *See Doe v. United States*, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992). According to the Advisory Committee Notes that accompanied this rule when it was first proposed, this standard was adopted for reasons of practicality. While strictly speaking the original of a photograph might be thought to be only the negative, practicality and common usage require that any print from the negative be regarded as an original. Similarly, practicality and usage confer the status of original upon any computer printout. Advisory Committee Notes, Proposed Federal Rule of Evidence 1001(3) (1972).

2. Computer Printouts as "Summaries"

Federal Rule of Evidence 1006 permits parties to offer summaries of voluminous evidence in the form of "a chart, summary, or calculation" subject to certain restrictions. Agents and prosecutors occasionally ask whether a computer printout is necessarily a "summary" of evidence that must comply with Fed. R. Evid. 1006. In general, the answer is no. *See Sanders*, 749 F.2d at 199; *Catabran*, 836 F.2d at 456-57; *United States v. Russo*, 480 F.2d 1228, 1240-41 (6th Cir. 1973). Of course, if the computer printout is merely a summary of other admissible evidence, Rule 1006

will apply just as it does to other summaries of evidence.

ABOUT THE AUTHOR

Orin S. Kerr is a Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice.