

September 1, 2000

Thomas J. Colson, Esq.
IP.com
c/o Manning & Napier Information Services
1100 Chase Square
Rochester, N.Y. 14604

**Privileged and Confidential
Attorney-Client Communication
Prepared in Contemplation
of Potential Litigation**

**Re: Study Regarding IP.com Defensive Publication Service
Our Ref.: 55653-010**

Dear Mr. Colson:

You have requested McDermott, Will & Emery's opinion on the following issues: (1) whether invention disclosures available on the IP.com website on the World Wide Web are authenticable, (2) whether such disclosures satisfy the hearsay rule or one of its exceptions, and (3) whether such disclosures satisfy the requirement of an original in a patent infringement action in federal district court in connection with an assertion of invalidity predicated on anticipation or obviousness under 35 U.S.C. §§ 102 or 103, respectively.

In preparing this opinion, we have conducted a detailed study of the law concerning the authentication and admissibility of documentary evidence in federal district court. We have also carefully reviewed the information provided to us by yourself and Sam Baxter, as well as our discussions with both of you concerning the IP.com defensive publication service. That information has been confirmed current as of August 18, 2000. Our opinion follows.

Executive Summary

Invention disclosures available on IP.com's website can be authenticated, satisfy the hearsay rule or one of its exceptions, and satisfy the requirement of an original in a patent infringement action in federal district court in connection with an assertion of invalidity under 35

Thomas J. Colson, Esq.
September 1, 2000
Page 2

IP.com Defensive Publication Service
Privileged and Confidential
Attorney-Client Communication
Prepared in Contemplation
of Potential Litigation

U.S.C. §§ 102 and/or 103. Witnesses from IP.com can provide testimony to authenticate the documents and to lay a foundation for the business records exception to the hearsay rule. A duplicate of the original invention disclosure submitted by the author and/or inventor will likely satisfy the requirement of an original since the authentication requirement will already have been satisfied.

TABLE OF CONTENTS

IP.com's Defensive Publication Service	4
Legal Standards	8
A. Requirement of Authentication or Identification	8
B. Hearsay Rule and Its Exceptions	10
1. The Hearsay Rule	10
2. The Business Records Exception	11
C. Requirement of an Original: The Best Evidence Rule	15
Analysis	16
A. The Disclosure Must be Authenticated or Identified	16
B. The Invention Disclosure and Its Date and Time Stamp are Likely Admissible Under the Hearsay Rule and the Business Record Exception	19
1. Although the Content of the Disclosure is Not Hearsay, the Date Specified in the Bibliographic Information Would Likely be Hearsay	19
2. The Date Specified in the Bibliographic Information Likely Meets the Business Records Exception to the Hearsay Rule	20
Conclusion	27

IP.com's Defensive Publication Service

IP.com will provide a defensive publication service. Invention disclosures will be submitted to IP.com. In return for a fee, IP.com will store the disclosures in a computer database, give each disclosure a unique disclosure identification ("a fingerprint"), make them available and searchable via the World Wide Web (*i.e.*, the Internet), and have them digitally notarized by a third-party outside vendor (*e.g.*, Surety.com) to indicate the date and time the disclosure is first searchable via the Internet.¹ The objective of IP.com's defensive publication service is to provide a service that ensures a disclosure is both a "printed publication" under the patent statute (35 U.S.C. § 101 *et seq.*)² and admissible at trial in a federal district court, so that parties attempting to invalidate a patent may utilize the IP.com website as a prior art database.

The publication process begins when an author and/or inventor electronically submits an invention disclosure. The "invention disclosure" consists of a primary document (*e.g.*, technical paper, invention description, etc.), attachments (*e.g.*, drawings, charts, tables, etc.), and bibliographic information (*e.g.*, preparer and/or inventor, English title and abstract, country of origin, etc.) to IP.com's primary server.³ A fingerprint is calculated for the primary document and each attachment associated therewith. A fingerprint is a linear combination of letters, numbers and symbols comprising numerous digits which cannot be replicated with any realistic expectation of success. IP.com then scans the files for viruses and unacceptable vocabulary

¹ We have not rendered an opinion on the authentication and admissibility of documents notarized by such notarization vendors.

² We have also not rendered an opinion on whether such invention disclosures satisfy the "printed publication" requirement.

³ The disclosure is submitted with the use of a document publication wizard in conjunction with a web browser using either HTTP or FTP protocol. IP.com prefers that a secure protocol such as HTTPS or secure FTP client is used.

(*e.g.*, profanity), internally indexes the bibliographic information, and extracts searchable text through a READ-ONLY process wherein the documents are opened in a READ-ONLY format and are neither modified nor saved (with the original file name). The extracted information is “saved as” a different file which is sent to an outside vendor to index for full text searching.

Using Microsoft Word, for example, IP.com extracts an HTML rendered file of the disclosure. The HTML rendered file maintains as much of the original formatting as possible, although it is not necessarily intended to be a complete reproduction of the original disclosure. A fingerprint is then calculated for the HTML file. The HTML rendered file of the disclosure allows a user to view a portion (in some cases all) of the disclosure via the Internet. In addition, a copy of the original disclosure can be downloaded in its entirety for a fee. IP.com will maintain a log that keeps count of the number of times an HTML file is viewed, and a count of the number of times the actual disclosure document is downloaded. All fingerprints generated are stored in IP.com’s database and associated with a corresponding disclosure record. At this point, IP.com makes the disclosure searchable by bibliographic information on its website through its primary server, and the disclosure is considered published.

The bibliographic information is modified to include fields that store all the fingerprints generated by IP.com, as well as the publication date of the disclosure. Additionally, the publication date is stored in a searchable field. The primary document (together with any attachments) and the bibliographic information are combined into a ZIP file (or archive). The ZIP file is essentially a concatenation of the two (or more, if attachments are present) files because no actual data compression is performed. This minimizes the potential for data loss that can occur when compressing and decompressing data. IP.com gives each ZIP file a fingerprint using fingerprinting software provided by the notarization service. Accordingly, each ZIP file

has its own unique fingerprint based on its contents. If even one character changes in the disclosure, the altered ZIP file would result in a different fingerprint.⁴

IP.com maintains a secondary server which periodically "hits" IP.com's website to determine whether any new disclosures have become available and, when appropriate, downloads all newly-available corresponding ZIP files. The secondary server archives an electronic copy of the ZIP file and sends the fingerprint of the ZIP file to a notarization service provider, who, in turn, notarizes the fingerprint of the ZIP file and stores a record of the notarized fingerprint.⁵ The notarization service provider sends the notarization record to IP.com, where it is archived on the secondary server. Finally, the secondary server sends a copy of the notarization record to IP.com's primary server. IP.com will also generate and archive logs of the activities performed to publish each disclosure.

The secondary server will also perform "downstream" testing of the disclosures on the primary server. Specifically, the secondary server will periodically download each disclosure on the primary server and generate a new fingerprint. The new fingerprint is compared to the original fingerprint that has been archived in order to ensure that the disclosures are still available and have not been modified in any way.

⁴ IP.com employs at least two measures to ensure that at no point during the process is the disclosure altered. First, IP.com extracts the searchable text in a READ-ONLY format and does not even process the attachments to the disclosure. Second, for the reasons stated herein, the fingerprint ensures that the disclosure is not altered at any point during the process after the fingerprint has been assigned.

⁵ The notarization process relies on patented technology that is under the ownership of Surety.com. See U.S. patents 4,309,569; 5,136,646; 5,136,647; Re. 34,954; and 5,781,629. Neither the validity nor the content of these patents have been considered in rendering this opinion. At this point in the process, the notarization service provider has date and time stamped the fingerprint of the ZIP file.

Within approximately one week from the publication date, the disclosure is indexed by the full text search provider and available for full text search.⁶ The disclosure is now searchable by bibliographic information and full text for a minimum of 20 hours per day, 7 days per week. IP.com keeps track of both the number of times a disclosure is downloaded and overall up time of the IP.com website in an effort to show the disclosure was publicly available. IP.com has indicated that certain steps would be taken to verify continued access to its server.⁷

The information that is searched and/or accessed on the Internet is an HTML rendering of at least a portion of the disclosure (in some cases all) and its corresponding bibliographic information. Once a client determines a document to be relevant, a request must be submitted to IP.com in order to obtain the full disclosure. In response, a copy of the fingerprinted (and notarized) copy of the disclosure is transmitted to the user. IP.com does not provide public access to the database which stores fingerprinted copies of the disclosures.

A number of persons are involved in the IP.com publication process. Among them are the following: (1) an IP.com programmer responsible for IP.com's extraction of searchable terms and rendering of the searchable disclosure; (2) an IP.com employee utilizing the fingerprinting software; (3) an IP.com systems administrator responsible for making sure the website is online and operational; and (4) a third-party (outside) co-locator which has administrative access to IP.com's primary server. All of the foregoing have access to the content of submitted disclosures.⁸

⁶ This date is not formally recorded, although it can be. Further, we are unaware of the amount of time required by the full text search provider to actually complete this task.

⁷ At the present time, a final decision has not been made on exactly how this will be done. One possible solution is the use of a monitoring software, such as ipMonitor, that produces logs of server states and downtimes.

⁸ IP.com also employs a senior software engineer responsible for database design and administration, a JAVA and HTML program writer rendering graphics, and a graphics designer.

Legal Standards

Pursuant to 28 U.S.C. § 1338(a), federal district courts have exclusive jurisdiction over patent cases. The Federal Rules of Evidence (hereinafter, Rules or F.R.E.) govern evidentiary matters in the federal district courts. FED. R. EVID. 101. The following three prerequisites generally must be satisfied for any document to be admissible in a federal district court:⁹

1. The document must be authenticated or identified (F.R.E. 901);¹⁰
2. The document must not be hearsay, or it must satisfy one of the exceptions to the hearsay rule (F.R.E. 801-807); and
3. The document must satisfy the requirement of an original (F.R.E. 1001-1004).

The legal standards for each of the foregoing prerequisites will be discussed in turn.

A. Requirement of Authentication or Identification

The requirement of authentication or identification of a document is set forth as follows:

The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

None of the foregoing have access to either the content or date and time stamp of submitted disclosures.

⁹ This memorandum assumes that the content and subject matter of the particular invention disclosure at issue would be deemed relevant. *See* FED. R. EVID. 401 and 402.

¹⁰ The subscribing witness' testimony (*e.g.*, one who can independently attest to the author's creation of the document) is generally not required. *See* FED. R. EVID. 903.

FED. R. EVID. 901(a) (emphasis added). By way of illustration (not by limitation), the Rules give several examples of authentication or identification conforming with this requirement, such as: (1) testimony of a witness with knowledge (*i.e.*, testimony that a matter is what it is claimed to be); (4) distinctive characteristics and the like (*e.g.*, appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances); and (9) a process or system (*i.e.*, evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result).¹¹ Example (1) contemplates a broad range of testimony from a witness with personal knowledge sufficient to support the jury's finding that the matter is what its proponent claims it to be. *See* ADVISORY COMMITTEE NOTES to Rule 901 (1972 Proposed Rules). Similarly, the characteristics of the item offered itself (as set forth in Example (4)), considered in view of the circumstances, afford sufficient authentication or identification in a great variety of cases. *See id.* Finally, "Example (9) is designed for situations in which the accuracy of a result is dependent upon a process or system which produces it." *Id.* Judicial notice of that accuracy, in appropriate circumstances, may be taken. *Id.*

The foregoing Rules are applicable to computer-generated documents and documents stored in computer databases. *See, e.g., United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997) (testimony from FBI agent sufficient to establish authenticity of printouts of records kept on computer of defendant). The overarching principle of authentication is that the party offering the document adduce sufficient testimony to show that a jury could find that the document is what its proponent claims it to be. *See id.* (citing FED. R. EVID. 901(a)). The witness must be able to testify as to the origin of the printout. *First Nat'l Bank of Jefferson Parish v. M/V Lightning Power*, 851 F.2d 1543, 1548 (5th Cir. 1988).

¹¹ Extrinsic evidence of authentication or identification is not required for, *inter alia*, notarized documents (F.R.E. 902(8)) and documents affixed with trade inscriptions indicating ownership, control, or origin (F.R.E. 902(7)).

Since the authentication requirement, the hearsay rule, and the business record exception to the hearsay rule are designed to ensure reliability of the documents offered into evidence (*Munoz v. Strahm Farms, Inc.*, 69 F.3d 501, 503 (Fed. Cir. 1996) (The business records exception to the hearsay rule is designed to ensure the reliability of the business record.)), further discussion of the reliability of the disclosure is included in the discussion herein of the business records exception to the hearsay rule.

B. Hearsay Rule and Its Exceptions

1. The Hearsay Rule

Unless an exception applies, hearsay is not admissible for the truth of the matter asserted in federal court. FED. R. EVID. 802. Hearsay is defined as "a statement, other than one made by the declarant [i.e., person making the statement] while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801. However,

[i]f the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, then the statement is not hearsay ... The effect is to exclude from hearsay the entire category of "verbal acts" and "verbal parts of an act" in which the statement itself affects the legal rights of the parties or is a circumstance bearing on conduct affecting their rights.

ADVISORY COMMITTEE NOTES to Rule 803(c) (1972 Proposed Rules). In other words, if the statement is offered merely to prove that the statement was made and not to prove the truth of its content, the statement is not hearsay. *See, e.g., Jauch v. Corley*, 830 F.2d 47, 51-52 (5th Cir. 1987) (in connection with allegation of defamation, remarks made in newspaper article not hearsay because not offered to prove truth of remarks but simply that they were made).

2. The Business Records Exception

There are a number of exceptions to the hearsay rule, the most notable for purposes of this memorandum being the exception described in Rule 803(6). Under Rule 803(6), records of regularly conducted activity (or, a business record)¹² are not inadmissible under the hearsay rule (whether or not the declarant is available as a witness). A record of a regularly conducted activity is defined as follows:

A ... data compilation^[13] in any form ... made at or near the time by,^[14] or transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity to make the ... 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.

FED. R. EVID. 803(6). Rule 803(6) does not require that the "person with knowledge ... be able to produce, or even identify ... the person upon whose first-hand knowledge the ... data compilation was based." ADVISORY COMMITTEE NOTES to Rule 803(6) (1974 Enactment).

¹² The business whose record is offered need not be a party to the litigation. *Saks Int'l, inc. v. M/V "Export Champion"*, 817 F.2d 1011, 1013 (2d Cir. 1987).

¹³ The term "data compilation" includes electronic computer storage. ADVISORY COMMITTEE NOTES to Rule 803 (6) (1972 Proposed Rules).

¹⁴ The record (the computer input, not the computer output) must be made at or near the time the events or transactions recorded. *United States v. Sanders*, 749 F.2d 195, 198 (5th Cir. 1984). "[S]o long as the original computer data compilation was prepared pursuant to a business duty in accordance with regular business practice, the fact that the hard copy offered as evidence was printed for purposes of litigation does not affect its admissibility." *United States v. Hernandez*, 913 F.2d 1506, 1512-13 (10th Cir. 1990); see *United States v. Ross*, 33 F.3d 1507, 1517 n.17 (11th Cir. 1994).

A sufficient foundation for the introduction of such evidence will be laid if the party seeking to introduce the evidence is able to show that it was the regular practice of the activity to base such ... data compilations upon a transmission from a person with knowledge, e.g., ... in the case of a computer printout, upon a report from the company's computer programmer or one who has knowledge of the particular record system.

Id. "In short, the scope of the phrase 'person with knowledge' is meant to be coterminous with the custodian of the evidence or other qualified witness." *Id.* "Rule 803(6) imposes no requirement that a witness be a 'participant in a chain ... which produced the printouts.'" *Zayre Corp. v. S.M. & R. Corp.*, 882 F.2d 1145, 1150 (7th Cir. 1988). In fact, a qualified witness need not even be an employee of the business as long as he understands the process or system. *Id.* Nor need the attesting witness have been the computer programmer (*United States v. Linn*, 880 F.2d 209, 216 (9th Cir. 1989)) or the person who actually created the document (*United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991)).¹⁵ In fact, the witness need not even attest to the accuracy of the information in the record. *United States v. Whitaker*, 127 F.3d 595, 601 (7th Cir. 1997). The witness simply must have knowledge of the procedures used in creating and maintaining the computer records. *United States v. Goodchild*, 25 F.3d 55, 62 (1st Cir. 1994).

The business records exception applies to computer-generated documents, and documents stored in computer databases and posted on Internet websites. "It is well-settled that computer compilations may constitute business records for purposes of [Rule 803(6)] and may be admitted at trial if a proper foundation is established." *Croft*, 750 F.2d at 1364. The mere possibility that computer records may be altered does not present a bar to its admissibility. *United States v.*

¹⁵ There are numerous examples of witnesses, who did not personally prepare the document, authenticating computer printouts and laying the foundation for the business records exception for computerized records. *See, e.g., Whitaker*, 127 F.3d at 601 (FBI agent authenticated printouts or records obtained from defendant's computer); *United States v. Croft*, 750 F.2d 1354, 1364-65 (7th Cir. 1984)(foundation laid for business records exception for computer printouts by university director of payroll and benefits).

Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988). "Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program,^[16] as with inaccuracies in any other type of business records, [only affects] the weight of the printouts, not their admissibility." *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988).

"A party seeking to impeach the reliability of computer evidence should have sufficient opportunity to ascertain ... whether both the machine and those who supply it with data input and information have performed their tasks accurately." *United States v. Liebert*, 519 F.2d 542, 547 (3d Cir. 1975). Therefore, the witness authenticating the document and laying the requisite foundation must be sufficiently familiar with the process used to generate the computer printout in order to withstand a challenge to the reliability of the document.

Whether, and to what extent, authenticating and laying a foundation for the business records exception for computer-generated documents is more difficult than conventional documents remains unsettled. Federal courts continue to test and refine the application of the foregoing rules. The current trend, however, appears to suggest a readier acceptance of computer generated documents in view of the increasing use of computer databases in businesses. At least one federal court of appeals has held that it should be no more difficult to authenticate and lay the requisite foundation for such documents:

While the suggestion has been made that there are unique foundation requirements for the admission of computerized business records ... this court previously held that 'computer data compilations ... should be treated as any other record of regularly conducted activity.'

¹⁶ Periodic testing of the computer system may be shown as evidence of the computer systems' reliability (*United States v. Weatherspoon*, 581 F.2d 595, 598 (7th Cir. 1978)), but generally is not a prerequisite to admissibility (*Moore*, 923 F.2d at 915).

United States v. Vella, 673 F.2d 86, 90 (5th Cir. 1982). *Vella* specifically distinguished an earlier opinion from another federal court of appeals wherein the court held:

[T]he complex nature of computer storage calls for a more comprehensive foundation. Assuming properly functioning equipment is used, there must be not only a showing that the requirements of the Business Records Act [predecessor to the business records exception] have been satisfied, but in addition the original source of the computer program must be delineated, and procedures for input control including tests used to assure accuracy and reliability must be presented.

United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (referring to Federal Business Records Act as predecessor to business records exception expressed in Fed. R. Evid. 803(6)). *Scholle* cited with approval *United States v. Russo*, 480 F.2d 1228, 1241 (6th Cir. 1973), which describes what is involved in laying the necessary foundation under a more rigorous application of the authentication requirement and foundation for the business records exception to the hearsay rule:

[T]he foundation for admission of [computerized records] consists of showing the input procedures used, the tests for accuracy and reliability and the fact that an established business relies on the computerized records in the ordinary course of carrying out its activities. The [opposing] party then has the opportunity to cross-examine concerning company practices with respect to the input and as to the accuracy of the computer as a memory bank and retriever of information ... [T]he court [must] 'be satisfied with all reasonable certainty that both the *machine*^{17]} and *those who supply its information*^{18]} have performed their functions with

¹⁷ Wide acceptance and use of a computer program is evidence of its trustworthiness and authenticity. *See, e.g., United States v. Casey*, 1996 C.C.A. LEXIS 406, at *8 (U.S. Navy-Marines Ct. Crim. App. Dec. 27, 1996) (errors in computer records due to incorrect data entry or operation of computer program go to weight and not admissibility because BAMS/UNIX computer systems are widely used and accepted both within and without the government).

¹⁸ The reliability and authenticity of computer records may be questioned to the extent that data entry and maintenance requires significant selection, correction and interpretation. *See Potamkin Cadillac Corp. v. B.R.I. Coverage Corp.*, 38 F.3d 627, 633 (2d Cir. 1994).

utmost accuracy.' ... [T]he trustworthiness of the particular records should be ascertained before they are admitted and ... the burden of presenting an adequate foundation for receiving the evidence should be on the parties seeking to introduce it rather than upon the party opposing its introduction.

480 F.2d at 1241 (referring to Federal Business Records Act hearsay exception) (emphasis added). Even though the application of *Scholle* and *Russo* appear to be of some questionable authority given the greatly increased acceptance of computer-generated documents since the times they were decided, the documents in question herein would appear to meet their more stringent application of authentication standards.

C. Requirement of an Original: The Best Evidence Rule

The Rules also require the "original" to prove the content of a writing or recording.¹⁹ FED. R. EVID. 1002. "If data are stored in a computer or similar device, any printout ... shown to reflect the data accurately, is an 'original'." FED. R. EVID. 1001(3).

¹⁹ A writing or recording consists of a data compilation. FED. R. EVID. 1001(1).

Analysis

A court might require IP.com to present the testimony of witnesses who can authenticate the invention disclosure, and lay the foundation for the admissibility under the hearsay rule and its exceptions, as well as the best evidence rule. In such a case, a person familiar with, and responsible for, IP.com's publication process would probably be required to testify.

A. The Disclosure Must be Authenticated or Identified

A witness from IP.com should be prepared to testify that the disclosure, as well as the date and time stamp used to verify the disclosure's the date of first public availability, are as the proponent (*i.e.*, the accused infringer) of the disclosure claims them to be. *See* FED. R. EVID. 901(a). In other words, the witness should be prepared to testify that the process in place at IP.com generated the disclosure content proffered and made the disclosure available to the public as of the date and time alleged.

The disclosure and its date/time stamp can be authenticated by a witness from IP.com who is familiar with the publication process. In order to ensure that the authentication requirement is met, IP.com should adequately prepare such a witness to be able to attest that both (1) the system (*i.e.*, primary and secondary servers) functioned properly and (2) the procedures in place at IP.com were followed by IP.com employees involved in the publication process in order to ensure that the disclosure had certain content as of the date and time specified in its accompanying bibliographic information.²⁰ *See Scholle*, 553 F.2d at 1125; *Russo*, 480 F.2d at 1241.

²⁰ Although the witness is testifying that the disclosure had certain content, this content is not examined in the traditional contextual manner. Rather, the content is examined in terms of the fingerprint produced by the disclosure.

With regard to element (1), the IP.com witness should be sufficiently familiar with the computer system used to receive and publish invention disclosures (i.e., make them available and searchable via the Internet). This would include overall system hardware architecture (e.g., primary and secondary servers) and software implemented (e.g., visual basic, HTML programming, and especially the fingerprinting software).²¹

With regard to element (2), the witness should be prepared to offer testimony concerning all details of IP.com's publication process, from start to finish, as set forth above. The witness should start from invention disclosure submission and conclude with publication and eventual tracking of document downloads. To the extent that IP.com employees play a part in the publication process, that part should be described. For example, the witness should be prepared to testify essentially to the following:

1. The disclosure was submitted to IP.com.
2. A fingerprint of the primary document was produced.
3. A fingerprint of each attachment was produced.
4. The searchable text is extracted and sent to an outside vendor for indexing.
5. An HTML rendered file of the disclosure is generated and fingerprinted.
6. The bibliographic information is modified to include the fingerprints produced in (2), (3), and (5) as well as the publication date of the document.
7. IP.com indexes the bibliographic information and makes the disclosure searchable by bibliographic information on its website through its primary server (i.e., publishes the document).
8. The primary document, the attachments, and the bibliographic information (including the date and time of the disclosure's first availability on the IP.com website) are combined into a ZIP file.
9. The ZIP file is given a fingerprint.
10. Each ZIP file has its own unique fingerprint—if even one character is changed, the fingerprint for the file would change.
11. A secondary server "hits" the IP.com website, downloads, and archives a copy of the ZIP file.

²¹ The witness could bolster the showing of accuracy by testifying that IP.com has an established practice of periodically testing the system to establish its reliability. *See Weatherspoon*, 581 F.2d at 598.

12. The secondary server sends a copy of the ZIP file's fingerprint to a notarization service provider.
13. The notarization service provider notarizes the fingerprint, stores a notarization record and sends a copy of the notarization record to IP.com's secondary server.
14. The secondary server, in turn, sends a copy of the notarization record to IP.com's primary server.
15. As soon as the disclosure is indexed by the full text search provider, it is made available for full text search.
16. The secondary server performs downstream testing to ensure that disclosures on the primary server are available and unchanged.
17. IP.com keeps track of the number of times an HTML file is accessed and the number of times a disclosure is downloaded.
18. IP.com maintains a log of all transactions performed in publishing a disclosure.
19. IP.com monitors overall up time of the IP.com website.
20. At no time do visitors to IP.com's website have access to the notarized fingerprint.

An important portion of this testimony are the steps taken to ensure that disclosures cannot be manipulated and/or altered in any way after it is given a fingerprint and notarized. To rebut an express or implied charge that the disclosure content was altered after the date and time assigned to it, or alternatively, that the date and time assigned to the disclosure was altered, the witness should be prepared to testify why this cannot happen in the IP.com publication process. In this regard, the witness should be familiar with what a fingerprint is (*i.e.*, how it uniquely identifies a document) and why it would change if any of the disclosure content or its bibliographic information (including date and time of first availability) was changed.²² The witness should also be prepared to discuss the number of times IP.com checks the fingerprint of a disclosure during the publication process to minimize the possibility that a disclosure could be altered between the time it is submitted and the time it is notarized.

²² Additional testimony by the IP.com witness that the notarization service provider itself date and time stamped a fingerprint of the ZIP file during the notarization process may bolster the authentication of the date and time stamp given the disclosure. The witness could testify that the date and time of the notarized record is very close in time to the date and time stamp specified in the bibliographic information given to the disclosure by IP.com.

B. The Invention Disclosure and Its Date and Time Stamp are Likely Admissible Under the Hearsay Rule and the Business Record Exception

The content (*i.e.*, the subject matter) of the disclosure would not be hearsay because it would not be offered to prove the truth of the matter asserted. In other words, the subject matter of the various publications available from IP.com would fall under this category because their importance as prior art rests on their accessibility by those of ordinary skill in the art. There is no need to show that the contents of the disclosures are actually true. The date and time specified in the bibliographic information, however, must fall within one of the hearsay exceptions if offered to prove that the disclosure was first made available on IP.com's website as of that date and time. To show this, testimony of a witness from IP.com could be used to lay a foundation for the business records exception to the hearsay rule.

1. Although the Content of the Disclosure is Not Hearsay, the Date Specified in the Bibliographic Information Would Likely be Hearsay

The content of the invention disclosure itself would not be hearsay because it would not be offered to prove the truth of the matter asserted. "A prior art document submitted as a 'printed publication' under 35 U.S.C. § 102(a) is offered simply as evidence of what it describes, not for proving the truth of the matters addressed in the document." *Joy Techs. v. Manbeck*, 751 F. Supp. 225, 233 n.2 (D.D.C. 1990), *aff'd*, 959 F.2d 226 (Fed. Cir. 1992). In *Joy Techs.*, the court received into evidence an industry publication, overruling a hearsay objection, and ascribed to it the same weight as every other prior art reference submitted, including a U.S. patent. *Id.* Similarly, a printed publication offered to render a U.S. patent invalid under 35 U.S.C. § 102(b) is not hearsay. *Freeman v. 3M*, 675 F. Supp. 877, 884 n. 5 (D. Del. 1987). *See also Abbott Labs. v. Diamedix Corp.*, 969 F. Supp. 1064, 1067 n.1 (Fed. Cir. 1997) ("[T]he [prior art] reference is being offered ... not to prove the truth of the matter asserted. The relevance of the document is

its very existence ... As such it is not hearsay."). In *Freeman*, the court held that the extract of a record from a clinical conference is not hearsay because the description need not have been true. *Id.* In view of the foregoing, if the invention disclosure submitted to IP.com is offered as a prior art printed publication,²³ its content would not be hearsay because it is not being offered to prove the truth thereof.

The date and time specified in the bibliographic information, however, would be hearsay if offered to prove that the disclosure was first made available on IP.com's website as of that date and time. Indeed, this would meet the definition of hearsay; namely, a statement not made at the trial or hearing, offered into evidence to prove the truth of the matter asserted. *See* FED. R. EVID. 801. The disclosure would have to be introduced under one of the exceptions to the hearsay rule.

2. The Date Specified in the Bibliographic Information Likely Meets the Business Records Exception to the Hearsay Rule

The publication would likely meet the business records exception to the hearsay rule. The same IP.com executive or employee who presented testimony to establish the authenticity of the disclosure can also present testimony required to lay the foundation for this exception since he/she understands the IP.com publication process. *See Zayre Corp.*, 882 F.2d at 1150. It does not matter that this person did not create the disclosure or the software program implemented to run the system. It is sufficient that they have knowledge of the routine procedures used by the system in generating and maintaining the disclosures on the Internet. *See Goodchild*, 25 F.3d at 62 (manager of fraud unit of credit card company qualified to testify as to records of telephone conversations made in the regular course of business even though he did not make the records himself or participate in telephone conversations).

²³ It is well known that prior art for purposes of 35 U.S.C. § 102 is prior art for purposes of 35 U.S.C. § 103.

The testimony of the witness laying the foundation for this exception would, in almost all respects, mirror the testimony given with regard to authentication. The witness should testify that after the disclosure was submitted to IP.com, fingerprints were generated for various files and searchable text was extracted for indexing by an outside vendor. Then, IP.com created an HTML rendered file of the disclosure and generated a fingerprint for the HTML file. Next, the bibliographic information was indexed to allow searching of disclosures by bibliographic information on IP.com's website through its primary server.

The primary document file, any attachments, and the bibliographic information (which includes the date and time of the disclosure's first availability on the IP.com website) were combined into a ZIP file. Importantly, the ZIP file is not compressed, but rather generated in the form of a concatenation of the files archived therein in order to eliminate data loss that can result from the compression process. The ZIP file was given a fingerprint, which is a linear combination of letters, numbers and symbols comprising numerous digits. Each ZIP file has its own unique fingerprint—if even one character is changed, the fingerprint for the file would change. Further, it is not possible to predict how a fingerprint would change if the document is altered.

The publication process requires that a secondary server "hit" the IP.com website and download a copy of the ZIP file created. A copy of the ZIP file's fingerprint is then sent to the notarization service provider. The notarization service provider notarizes the fingerprint, stores a notarization record, and sends a copy to IP.com's secondary server. The secondary server, in turn, sends a copy of the notarization record to IP.com's primary server. Finally, the witness would have to testify that within approximately one week, the disclosure was indexed by the full text search provider and made available for full text searching over the Internet. However, the disclosure title and abstract (which are always in English) were searchable as soon as the disclosure was published.

The witness should be able to testify that the foregoing process is the routine business practice of IP.com, and that logs of all transactions performed to publish a disclosure, as well as all related fingerprints, are generated and archived. The Court of Appeals for the Federal Circuit, which handles all appeals in patent infringement cases, in analogous circumstances has held that evidence of routine business practice can be adduced to show that a document was made available as of a certain date. In determining when certain references were publicly available so as to constitute "printed publications" under the patent statute, the Court has stated:

The statutory phrase "printed publication" has been interpreted to mean that before the critical date the reference must have been sufficiently accessible to the public interested in the art; dissemination and public accessibility are the keys to the legal determination whether a prior art reference was "published." ... [The defendant] presented extensive uncontroverted evidence of business practice that was sufficient to prove that [the reference] was widely available and accessible to the interested public before [a certain date]. *Evidence of routine business practice can be sufficient to prove that a reference was made accessible before a critical date.* Accessibility goes to the issue of whether interested members of the relevant public could obtain the information if they wanted to. If accessibility is proved, there is not requirement to show that particular members of the public actually received the information.

Constant v. Advanced Micro-Devices, Inc., 848 F.2d 1560, 1568-69 (Fed. Cir. 1988) (emphasis added and internal citations omitted). *Constant* made reference to an earlier Federal Circuit decision, *In re Hall*, 781 F.2d 897 (Fed. Cir. 1986), which held that the testimony of the director and manager of the loan department at a university library in Germany²⁴ established the library's

²⁴ The disclosures on IP.com's would not fail to be "printed publications" within the meaning of 35 U.S.C. §§ 102(a) and 102(b) simply because they may not be in English. Neither § 102(a) nor § 102(b) explicitly require that the "printed publication" be in English. Indeed, the Federal Circuit has implicitly held that publications not in English can constitute printed publications within the meaning of §§ 102(a) and 102(b). *See, e.g., Titanium Metals Corp. v. Banner*, 778 F.2d 775 (Fed. Cir. 1985) (claims in patent application invalid under §§ 102(a) and 102(b) as anticipated by Russian article). Further, the Federal Circuit's predecessor specifically stated that all foreign language and English printed publications are "treated the same for prior art purposes under § 102." *In re Howarth*, 654 F.2d 103, 107 (C.C.P.A. 1981). *In re Hall*, *supra*, involved a

general practice for indexing, cataloguing, and shelving theses and the time it would generally take to make a thesis available to the interested public after it was received from the author. 781 F.2d at 899. The Federal Circuit stated:

[The Court has not held] that accessibility can only be shown by evidence establishing a *specific* date of cataloguing and shelving before the critical date. While such evidence would be desirable, in lending greater certainty to the accessibility determination, the realities of routine business practice counsel against requiring such evidence. The probative value of routine business practice to show the performance of a specific act has long been recognized ... Therefore, we conclude that competent evidence of the general library practice may be relied upon to establish an approximate time when a thesis became accessible.

Id.

To borrow from the analogy above, the witness can testify that it was the routine business practice of IP.com to include the date the disclosure was first made available on its website in the bibliographic information. In turn, that bibliographic information, along with the primary document of the content of the disclosure, was included in a ZIP file, that was fingerprinted and notarized. Indeed, *In re Hall* would suggest that IP.com need not conclusively establish that the disclosure was available on the date specified in the bibliographic information, but merely that it was available as of approximately that date.

thesis written by a student and made available at a German university. That decision by the Federal Circuit seems to suggest that the document must be searchable by bibliographic information such as author, title, and subject matter. 781 F.2d at 898-99. By making disclosures on its website searchable by such bibliographic information in English, IP.com increases the likelihood that the disclosure (even if not in English) is a printed publication as understood in §§ 102(a) and 102(b).

There have been concerns expressed regarding documents posted on the Internet.²⁵ These opinions appear to be distinguishable because the invention disclosures need not be admitted for the truth of the matter to qualify as prior art. Further, the computer records showing the date that the disclosure was received would be protected from tampering by the fingerprinting process. In connection with the business records exception, IP.com will not be relying on the Internet service provider as the business whose records are maintained on its website. Nor will visitors to the website be able to alter the content and corresponding date and time stamp of a disclosure since the ZIP files (which include that information) are fingerprinted.

In circumstances analogous to those under consideration here, the Federal Circuit has held that dated slide frames satisfy the business records exception to the hearsay rule. *Munoz v. Strahm Farms, Inc.*, 69 F.3d 501, 503 (Fed. Cir. 1996). In *Munoz*, a farm adviser associated with the University of California took photographs of harvesting operations and use the slides for teaching purposes. *Id.* at 502. The Federal Circuit held that a foundation for the business records exception was established by testimony of the custodian of the slides that it was his practice to send film to Kodak for processing and check the dates for developed slides. *Id.* It did not matter that he himself had not placed the dates on the slides since a custodian of the record need not have created the record. *Id.* The Federal Circuit therefore affirmed the district court's admission of the dated slides into evidence under the business records exception to the hearsay

²⁵ A recent federal court of appeals decision held web postings inadmissible hearsay not entitled to the business records exception. *United States v. Jackson*, 208 F.3d 633, 637-38 (9th Cir. 2000). The defendant in *Jackson* offered web postings from an Internet web site in her defense, arguing that they fit the business records hearsay exception as business records of the Internet service provider. *Id.* at 637. The court of appeals affirmed the trial court's exclusion because the Internet service provider was merely the conduit of the information, did not post the content, and there was no evidence that it monitored the content. *Id.* "The fact that the [Internet] service providers may be able to retrieve information that its customers posted or email that its customers sent does not turn that material into a business record of the Internet service provider." *Id.*

rule. *Id.* The slides were then adduced to show that a device in use pre-dated and invalidated the patent asserted under 35 U.S.C. § 102(b). *Id.*

Similarly, IP.com could adduce the testimony of a person with knowledge of its defensive publication process. The witness could testify it was the established business practice to date and time stamp disclosures as of first availability on its website, in accordance with the procedures outline above.

Some question, however, may be raised as to whether the disclosure itself (as opposed to its content) is indeed the record of a regularly conducted business activity as traditionally applied under Rule 803(6). Although IP.com may not necessarily generate "business records" in the traditional sense by making invention disclosures available on its website (*compare Catabran*, 836 F.2d at 457 (admitting computer printout of business' general ledger based on testimony of person who input data and checked the accuracy of calculated results)), it nevertheless has every incentive and interest in ensuring the accuracy of the content and date stamp given the disclosure as of first publication. Indeed, ensuring that accuracy *is* its business. In this regard, it must be kept in mind that the witness' testimony need only satisfy the threshold showing that the exception applies, and the ultimate question as to the document's accuracy goes to its weight, not its admissibility. *See Scholle*, 553 F.2d at 1125 ("[A]lthough the foundation for reception of the evidence could have been more firm we cannot say that the trial court erred in admitting it. Any evidentiary shortcoming thereafter became a matter of weight to be given the evidence rather than one of admissibility."). Decisions such as *Munoz*, *supra*, show that federal courts are unlikely to limit application of the business records exception to a traditional notion of a business record.

By authenticating the disclosure and laying the foundation for the business records exception to the hearsay rule, the witness will have per force established that the printout of the disclosure reflects the data accurately. In other words, the printout will have been shown to

accurately reflect the content and the date of first availability on the IP.com website, thus satisfying the best evidence rule.²⁶

²⁶ Demonstration of the fingerprinting software, *i.e.*, generating a fingerprint of the disclosure and its bibliographic information (including date and time stamp), and showing it matches the notarized fingerprint sent by the notarization service provider, would bolster evidence of the printout's accuracy.

Conclusion

Based on the above analysis, it is our opinion that invention disclosures made available on IP.com's website can be authenticated, satisfy the hearsay rule or the business records exception, and satisfy the requirement of an original in a patent infringement action in federal district court in connection with an assertion of invalidity under 35 U.S.C. §§ 102 and/or 103.

Notwithstanding this opinion, we cannot, of course, guarantee that a party will not challenge the authentication and admissibility of invention disclosures available on the IP.com website. Nor can we guarantee that a party will not allege that such disclosures are not "printed publications" under the patent statute. However, we believe that a properly informed court (or other fact finder) should agree with the opinions expressed above.

As is the policy of McDermott, Will & Emery, this opinion has been reviewed by two partners in our firm, Mark G. Davis and Jack Q. Lever, both of whom agree in substance with the conclusions stated.

Very truly yours,

McDermott, Will & Emery

JQL:MGD:LDT:CDB/djf
Enclosures

cc: R.V. Lupo, Esq. (w/enclosures)