Paper No. 20

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Dolby Laboratories, Inc.

Petitioner,

v.

Intertrust Technologies Corporation,

Patent Owner.

Case IPR2020-00660
Patent No. 6,785,815

PATENT OWNER'S RESPONSE PURSUANT TO 37 C.F.R. § 42.120

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutory Authorities

Rules and Regulations

EXHIBIT TABLE

Exhibit #	Description
2001	[INTENTIONALLY LEFT BLANK]
2002	[INTENTIONALLY LEFT BLANK]
2003	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC, Dkt. No. 61-3 (N.D. Cal. Nov. 27, 2019): Second Amended Complaint (Public Version)
2004	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case), Dkt. No. 95 (E.D. Tex. May 5, 2020): First Amended Docket Control Order
2005	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case), Dkt. No. 8 (E.D. Tex. Oct. 21, 2019): Consolidation Order
2006	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case), Dkt. No. 22 (E.D. Tex. Nov. 7, 2019): Consolidation Order
2007	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case), Dkt. No. 112 (E.D. Tex. July 7, 2020): Claim Construction Order
2008	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC, Dkt. No. 73 (Feb. 13, 2020): Case Management and Pretrial Order For Claims Construction
2009	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC, Dkt. No. 71 (Feb. 6, 2020): Joint Case Management Conference Statement
2010	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case) (E.D. Tex. January 30, 2020): Defendants' Invalidity and Subject Matter Eligibility Contentions
2011	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case), Dkt. No. 78 (E.D. Tex. April 17, 2020): Order Appointing Technical Advisor
2012	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC (April 13, 2020): Dolby's Invalidity Contentions Pursuant to Patent Local Rule 3-3 and 3-4

2013	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case) (E.D. Tex. January 30, 2020): Defendants' Invalidity Claim Charts For The '815 Patent - Appendices C-03 (Hanna), C-04 (Gennaro), C-07 (Stefik), and C-Combination (showing Section 103 combinations for the '815 patent)
2014	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC (April 13, 2020): Exhibit C-03 - Dolby's Invalidity Contentions For The '815 Patent Based on Hanna
2015	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC (April 13, 2020): Exhibit C-04 - Dolby's Invalidity Contentions For The '815 Patent Based on Gennaro
2016	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC (April 13, 2020): Exhibit C-07 - Dolby's Invalidity Contentions For The '815 Patent Based on Stefik
2017	[INTENTIONALLY LEFT BLANK]
2018	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case) (E.D. Tex. November 6, 2019): Intertrust's Patent Rule 3-1 Disclosures - Infringement Contentions For The '815 Patent
2019	*Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, Case No. 2:19-cv-00266-JRG (lead case), Dkt. No. 28, (E.D. Tex. November 6, 2019): Defendants' Motion to Transfer Venue to N.D. Cal.
2020	[INTENTIONALLY LEFT BLANK]
2021	[INTENTIONALLY LEFT BLANK]
2022	[INTENTIONALLY LEFT BLANK]
2023	*Dolby Laboratories, Inc. v. Intertrust Corporation*, Case No. 3:19-cv-03371-EMC, Dkt. No. 101 (August 12, 2020): Order on Joint Stipulation Regarding Claim Terms and Claim Construction Schedule
2024	Declaration of Dr. Vijay K. Madisetti, IPR 2020-00663 (May 27, 2020)
2025	U.S. Patent No. 5,892,900
2026	Deposition Transcript of Dr. Vijay K. Madisetti (January 5, 2021)

2027	Declaration of Dr. Markus Jakobsson
2028	"On the Security of Public Key Protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208 (1983)
2029	"Tamper Resistant Software: An Implementation", *Proceedings of the First International Workshop on Information Hiding*, p. 317–333 (May 1996)
2030	"Discouraging Software Piracy Using Software Aging", *ACM Workshop on Digital Rights Management* (February 2002)

Dolby Laboratories Inc.'s ("Petitioner" or "Dolby") Petition (Paper 2, "Petition" or "Pet.") asserts two grounds based on pre-AIA 35 U.S.C. §103(a) for invalidity of claims 42-43 of U.S. Patent 6,785,815 ("'815 patent") that is assigned to Intertrust Technologies Corporation ("Patent Owner" or "Intertrust"): (1) obviousness over PCT Publication WO 99/40702 ("Hanna") in view of U.S. Patent No. 5,629,980 ("Stefik") (Pet. at 19-41); and (2) obviousness over U.S. Patent No. 6,009,176 ("Gennaro") (Pet. at 42-59).

Petitioner has not met its "burden of proving a proposition of unpatentability by a preponderance of the evidence." 35 U.S.C. § 316(e). The Petition should be denied for several reasons.

The '815 patent is in the field of digital piracy prevention and/or digital rights management ("DRM"), and is concerned with preventing a user from being able to circumvent controls that prohibit or restrict the use of protected content. Thus, it discloses inventive systems and methods that seek to prevent unauthorized access and use of protected content, while allowing users to play unprotected content without restriction. Methods such as the Challenged Claims that require a request to use a file in a predefined manner, and the granting of such a request, only make sense when the user (*i.e.*, the requester) poses a risk of accessing and using the data in an unauthorized manner. The two primary references that Petitioners rely on, Hanna and Gennaro, are in a different field, address different problems, and are not

concerned with risks posed by a user. To the contrary, they both seek to detect data corruption during transmission, either by unintentional network errors or malicious corruption by unknown third parties, before the corrupted data reaches a user. The Petition fails to show that a POSITA would be motivated to modify these transmission-related data corruption detection references by adding "the [receiving]/[grant] to use…in a predefined manner" process of the Challenged Claims because the transmitter of the content is not concerned about unauthorized use by the recipient.

The Board should deny the Petition because each of Petitioner's grounds fails to demonstrate by a preponderance of evidence that claims 42-43 are unpatentable. Regarding **the first ground**, Petitioner's primary reference, Hanna, is not prior art under 35 U.S.C. §102(a) because it was published on August 12, 1999, more than two months after the June 8, 1999 priority date of the Challenged Claims via a provisional application. Contrary to Petitioner's cursory analysis and conclusion, the 23-page, 12-drawing sheet provisional application clearly shows that the inventor was in possession of the claimed invention, providing written support for claims 42 and 43. Petitioner's first ground additionally fails because Hanna is not analogous art and fails to disclose at least two limitations of the Challenged Claims that govern the use of content: "receiving a request to use the file in a predefined manner" and "granting the request…." Petitioner also fails to provide a motivation to modify or

combine Hanna's transmission-related data corruption detection system with Stefik's purported teachings to achieve these claim limitations. Ground 1 should be denied.

With respect to **the second ground**, Petitioner fails to show that Gennaro discloses these same two limitations ("receiving a request to use the file in a pre-defined manner" and "granting the request"), and provides no evidence that a skilled artisan would modify a system for detecting transmission errors into one that manages the use of the data by the recipient. Gennaro makes no reference to "receiving" a request to use a file in a predefined manner, and Petitioner distorts Gennaro's teachings in its attempt to fabricate such a disclosure. Gennaro's data stream authentication protocol also does not perform a "granting" step in response to a request to use a file in a predefined manner, as required by the Challenged Claims. Instead, once processing begins, Gennaro's system allows processing of an individual block of a stream to continue if tampering is not detected; but if tampering is detected, further processing of that block is halted. Thus, the Petition impermissibly conflates the claimed *granting* of a request to use a *file* in a pre-defined manner with Gennaro's acquiescence in allowing the processing of authenticated blocks to continue so that they may eventually be used. Ground 2 should be denied.

For each of these reasons, Petitioner fails to meet its burden.

I. OVERVIEW OF THE '815 PATENT

A. The '815 Patent Specification

The '815 patent describes novel anti-piracy systems and methods for using digital signatures and watermarking techniques to control access to, and use of, data. Ex. 1001 at 1:23-27; Ex. 2027 at ¶76. It seeks to address two problems facing digital content creators. First, it observes that "[t]raditional content-distribution techniques offer little protection from piracy" and that "the threat of piracy has kept the market for digital goods from reaching its full potential." *Id*. at 1:41-43; ; Ex. 2027 at ¶77. Second, and relatedly, it recognizes that "[a]nother problem faced by content owners and producers is that of protecting the integrity of their electronic content from unauthorized modification or corruption" *Id*., 2:6-10; Ex. 2027 at ¶77.

The '815 patent seeks to prevent attackers from distributing and playing unauthorized copies of a digital work and "preserve the security of digital files by detecting unauthorized modifications." Ex. 1001 at 9:27-10:9; ; Ex. 2027 at ¶¶78-79. But the '815 patent is not concerned with preventing modifications to the content that is played (*e.g.*, a music track) because a pirate would not be incentivized to corrupt such data. See Ex. 1001 at 1:42-48 (digital technology "enables information to be ***perfectly reproduced*** at little cost"). Rather, the patent is concerned with preventing removal of anti-piracy data (*e.g.*, special codes or signed hash files) that the content creator may store with the related content for the purpose of, for example,

preventing use of the content on unauthorized devices. *Id*. at 9:52:57; 24:7-9 ("These signed hash files 1400 can be stored on CDs or other media ***along with the content to which the they relate***."); 24:32-34 ("content management module 1534 checks for a signed hash file 1514 ***corresponding to content*** 1530"); 23:58-62 ("a user 1524 who downloads a track 1510 from a server 1508 may obtain the ***corresponding file of signed hashes*** as part of the same transaction (or by separately connecting to server 1506).") (emphases added); Ex. 2027 at ¶80. The '815 patent describes that the "content management module uses the signed hash file 1514 to control access to the file as shown in FIG. 13," reproduced below. *Id*. at 24:43-45; Ex. 2027 at ¶81.

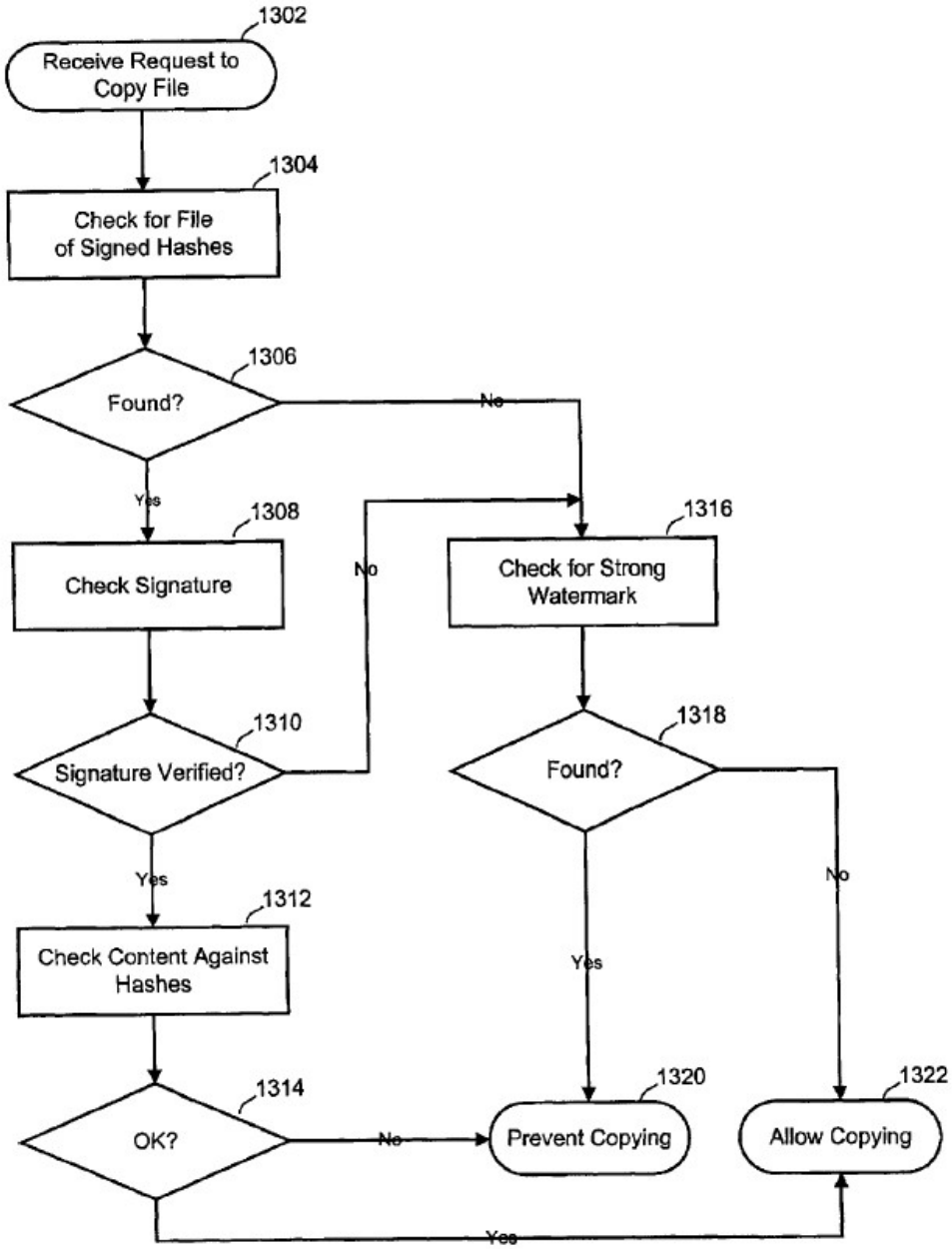

FIG. 13

The '815 patent also seeks to prevent attackers from adding special codes to an unprotected piece of content in order to, for example, "use the content on a device that checks for the presence of these codes as a precondition for granting access to

the content or for performing certain actions (*e.g.*, accessing the content more than a certain number of times, printing a copy of the content, saving the content to a memory device, etc.)." *Id*. at 9:57-63; ; Ex. 2027 at ¶82. Claims 42 and 43 of the '815 patent are two patented methods that may be used to detect unauthorized attempts to remove or add such encoding and prevent the circumvention of anti-piracy measures. Ex. 2027 at ¶82.

B. The '171 Provisional Application

The '815 patent claims priority to provisional application 60/138,171 ("'171 Application"), filed on June 8, 1999, which is incorporated by reference into the '815 patent. *See* Ex. 1001 at 1:6-11. The '171 Application discloses such a process for controlling access and use of proprietary data using signatures and watermarking techniques, as illustrated in the provisional application's annotated FIG. 6, below. *See* Ex. 2027 at ¶¶91-93.

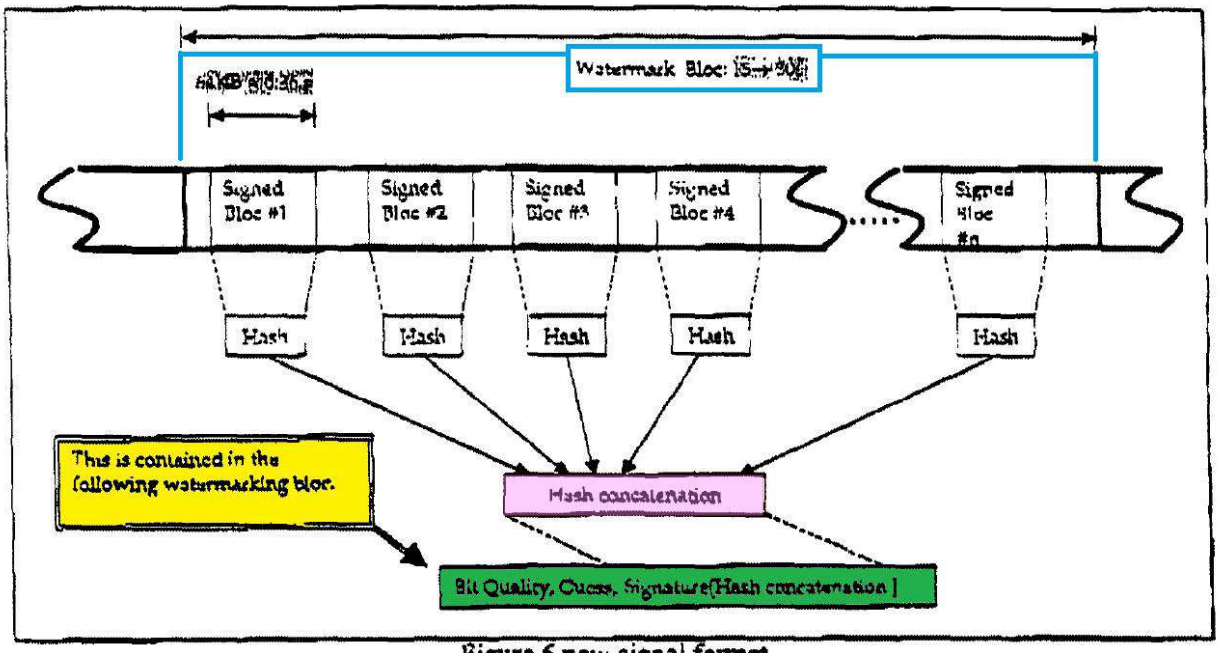

Figure 6 new signal format.

Specifically, the provisional application discloses a process that includes generating a signed hash concatenation by partitioning a signed data stream 602 (blue). Ex. 1004 at 20, FIG. 6; ; Ex. 2027 at ¶95. These partitions are hashed and the resulting hashes are concatenated to form a hash concatenation (pink), which is then signed. *Id.* FIG. 6 explains that the signed hash concatenation (green) "is contained in the following watermarking bloc[k]." Ex. 1004 at FIG. 6 (quoted text in yellow box). That is, a signed hash concatenation associated with a first data block is embedded in the watermark of the following data block in the transmission. In the "error-recoverable shared signature scheme" disclosed, "[i]f an error appears on the data, the signature will verify for all partitions except for the one that is

affected." Ex. 1004 at 20; Ex. 2027 at ¶96. Thus, the signed hash concatenation received in the watermark of the following data block is used to verify the preceding data block.

A POSITA would understand that, to proceed with verification of the signed hash concatenation, the system would first extract the signed hash concatenation from the watermark of the successive data block received. Ex. 2027 at ¶97. The signature (*i.e.*, the signed hash concatenation) would then be, for example, processed (*e.g.*, "decrypted" according to RSA protocols) to reveal the underlying hash concatenation. *Id*. As part of the verification process, the actual data block received is partitioned and hashed to obtain a hash concatenation so that a comparison can be made between the hash concatenation retrieved from the data block and the hash concatenation retrieved from the digital signature. *Id*.; s*ee also* Ex. 1004 at 20 ("If an error appears on the data, the signature will verify for all partitions except for the one that is affected."); *see also id.* at FIG. 2C (illustrating signature verification by comparing a hash of the data block received (*i.e.*, " X ") and a hash of the unsigned signature (*i.e.* " X' ")).

When the hash concatenation from the digital signature is compared to the concatenation of the hash values retrieved from the received data block, a match between the two verifies the authenticity concatenation of the hash values obtained from the received data block. Ex. 2027 at ¶99. The individual hashes that make up

the concatenation of hash values can then be used, one by one, to verify the authenticity of corresponding partitions of the data block received. *See* Ex. 1004 at 20 ("If an error appears on the data, the signature will verify for all partitions except for the one that is affected."); FIG. 6; Ex. 2027 at ¶99.

C. The '815 Patent Claims

While the '815 patent includes 46 claims, Petitioner only challenges independent claim 42 and dependent claim 43:

> 42. A method for managing at least one use of a file of electronic data, the method including:
>
> [a] receiving a request to use the file in a predefined manner;
>
> [b] retrieving at least one digital signature and at least one check value associated with the file;
>
> [c] verifying the authenticity of the at least one check value using the digital signature;
>
> [d] verifying the authenticity of at least a portion of the file using the at least one check value; and
>
> [e] granting the request to use the file in the predefined manner.
>
> 43. A method as in claim 42, in which the at least one check value comprises one or more hash values, and in which verifying the authenticity of at least a portion of the file using the at least one check value includes:
>
> hashing at least a portion of the file to obtain a first hash value; and
>
> comparing the first hash value to at least one of the one or more hash values.

D. Prosecution History of the '815 Patent

The '815 patent issued on August 31, 2004 from U.S. Application No. 09/588,652 ("'652 Application"), filed on June 7, 2000. As discussed above, the '652 Application claims priority to the '171 Application. The Examiner's "Reasons For Allowance" stated that he Challenged Claims (along with the other claims) included "uniquely distinct features" that were "not found in the prior art, either singularly or in combination." *See* Ex. 1003 at 145, 153.

II. OVERVIEW OF THE CITED ART

A. Hanna (Ex. 1006)

Hanna is directed to the field of transmission-related "data corruption detection" and purports to address "a need for a system that protects against unintentional data corruption and malicious acts that cause errors in data processing," Ex. 1006 at 3:1-4; Ex. 2027 at ¶¶125-127, 129, 134. It particularly seeks to solve the problem of high computational overhead associated with verifying "bulk signature[s]" applied to a complete data set that is transmitted. *See* Ex. 1006 at 1:5-8, 2:1-3:4; Ex. 2027 at ¶128. To address this problem, Hanna "create[s] a hierarchy of hash values that start with packet hashes of an arbitrary data set and culminate in a single signed block allow[ing] a single digital signature to protect the data set" from "errors in data processing." *Id.* at 3:6-8; Ex. 2027 at ¶130. "Receiving

this hierarchy of hashes before the data also allows the data packets to be quickly verified as they are received." *Id.* at 3:8-10.

Referring to FIG. 4 of Hanna below, Hanna's hierarchical hashing scheme includes dividing a sequence of data values 401 into groups of data packets 402a-f. Ex. 1006 at 10:26-27; Ex. 2027 at ¶131. A hash function is applied to each data packet group 402a-f to generate a hash block 404 consisting of hash values B_1-B_6. Ex. 1006 at 10:28-11:1; Ex. 2027 at ¶132. The resulting hash values are grouped themselves (404a, 404b) and hashed again to generate a higher level hash block 406. *See* Ex. 1006 at 11:2-8. The process continues until the resulting hash block (and associated signature) is small enough to fit within a single packet. *Id.* The highest level hash block 406 is then signed. *Id.* at 11:8-10. The hash blocks are all transmitted. *Id.* at 9:11-13.

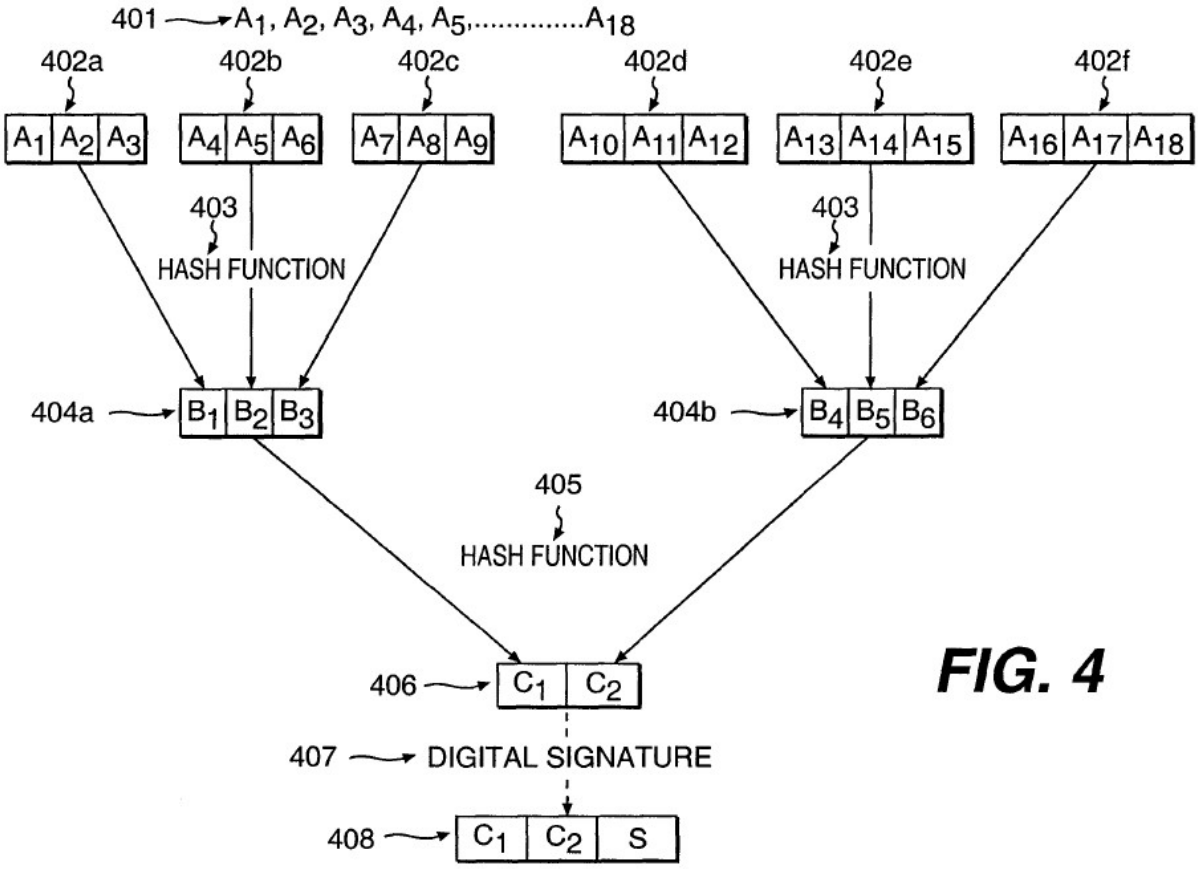

FIG. 4

Referring to FIG. 5 of Hanna below, data verification "begins with checking the digital signature on the top level hash block 502." Ex. 1006 at 11:12-13; Ex. 2027 at ¶133. If the top level hash block 502 passes the check, the next level hash 501 is verified by hashing the grouping of B_1-B_6 and comparing it to the higher level hash C_1. Ex. 1006 at 11:13-19. The data packets A_1-A_{18} are verified by comparing their hashes with the lowest level hash blocks. *See id.* at 24-29.

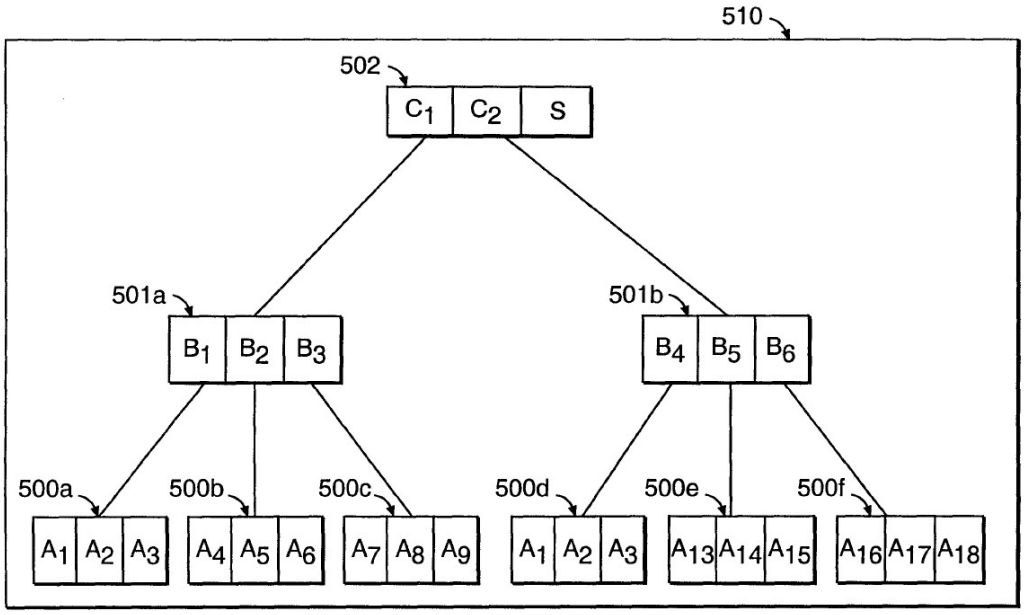

FIG. 5

B. Stefik (Ex. 1007)

Stefik is in the "field of distribution and usage rights enforcement for digitally encoded works," which places it, like the '815 patent, in the field of digital piracy protection and/or DRM. Ex. 1007 at 1:6-7; Ex. 2027 at ¶¶135-136. It is directed generally at the problem of preventing the unauthorized and unaccounted distribution or usage of electronically published materials, and, in particular, to the problem posed to such accounting systems when "the means for billing runs with the media rather than the underlying work." Ex. 1007 at 1:10-23, 3:40-47; Ex. 2027 at ¶137. In response, Stefik provides a system where the "owner of a digital work [] attach[es] usage rights to the work" that "define how it may be used and distributed." Ex. 1007 at 3:50-58; Ex. 2027 at ¶138.

Referring to FIG. 1 of Stefik below, a creator of a digital work determines the appropriate usage rights and fees, attaches them to the digital work, and stores the work in a first repository. Ex. 1007 at 7:6-11; Ex. 2027 at ¶¶139-140. The digital work remains stored in the first repository until a request for access is received from a second repository using a secure session. Ex. 1007 at 7:13-18.

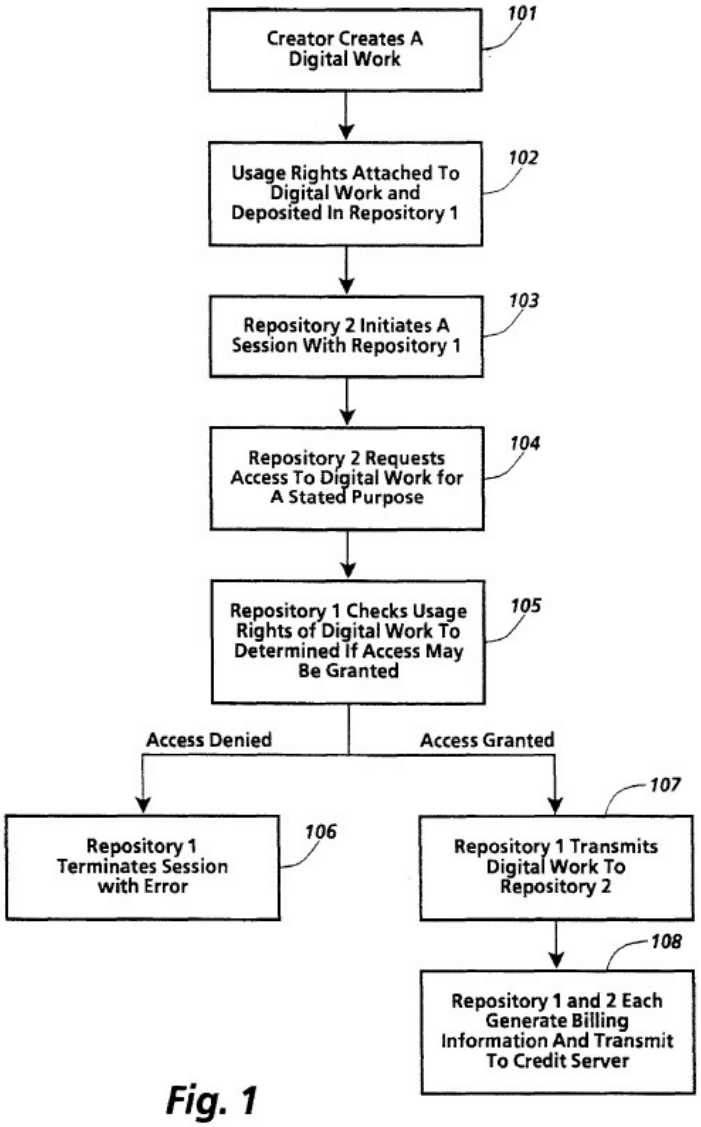

Fig. 1

The second repository may request access to the digital work for a stated purpose, for example, to print or to obtain a copy of the digital work. Ex. 1007 at 7:19-22; Ex. 2027 at ¶141. That purpose will correspond to a specific usage right. *Id.* at 7:22-23. The first repository checks the usage rights associated with the digital work to determine if the access to the digital work may be granted. *Id.* at 7:24-26. The check involves a determination of whether a right associated with the access request has been attached to the digital work and if all conditions associated with the right are satisfied. *Id.* at 7:26-29. If access is denied, the first repository terminates the session with an error message; otherwise, the repository transmits the digital work. *Id.* at 7:29-32.

C. Gennaro (Ex. 1008)

Gennaro, like Hanna, is directed to the field of transmission-related data corruption detection and describes a "method of signing and authenticating a stream of data using a reduced number of digital signatures." Ex. 1008 at 1:4-6; Ex. 2027 at ¶¶142-144. Gennaro describes how a data stream is divided up into a series of data blocks that each include a hash of the successive block in the stream. *See id.* at 4:14-58, FIG. 1A; Ex. 2027 at ¶145. The first block in the stream, which includes the hash of the second block in the stream, is then hashed and signed to generate authentication data consisting of a signature, hash, and size. Ex. 1008 at 4:59-65, FIG. 1B. The authentication data is then sent to the receiver before the data stream

is sent. *Id.* at 4:66-5:2. Gennaro emphasizes that one benefit of its invention is that the "receiver authenticates the stream without receiving the entire stream." *Id*. at 2:35-37.

Upon receipt of the authentication data, the receiver verifies the signature in the authentication data, and, if authentic, extracts the hash and size values in order to begin authenticating the received data stream. Ex. 1008 at 5:23-34; Ex. 2027 at ¶146. The data stream is split into blocks according to the size information received, and each block (after the first block) is authenticated or determined to be corrupt using the hash found in the preceding block. Ex. 1008 at 5:35-67.

III. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art ("POSITA") relevant to the '815 patent at the time of the invention would have a Bachelor of Science degree in electrical engineering and/or computer science, and three years of work or research experience in the field of digital piracy protection and/or DRM, or a Master's degree in electrical engineering and/or computer science and two years of work or research experience in that field. Ex. 2027 at ¶¶30-31. Petitioner's description of a POSITA is incorrect because, as Dr. Jakobsson explains, it defines the field of invention so broadly—

"electronic data protection and distribution"—as to be meaningless.[1] *See* Petition at 18; .Ex. 2027 at ¶¶32-51. Indeed, a person with the breadth of knowledge of the prior art ascribed to it by Petitioner's purported field of invention would be anything but one of ordinary skill.[2] *See In re GPAC Inc.*, 57 F.3d 1573, 1577–78, 35 U.S.P.Q.2d 1116 (Fed. Cir. 1995) (In determining obviousness, the scope of relevant prior art "necessarily encompasses not only the field of the inventor's endeavor but also any analogous art.") The ultimate positions set forth in this response regarding the validity of the Challenged Claims, however, would be the same under either parties' proposal.

IV. CLAIM CONSTRUCTION

Claim terms in an IPR are "construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. §282(b), including construing the claim in accordance with the ordinary and

[1] Dr. Madisetti refused to state whether the field of "electronic data protection and distribution" was subsumed by the field of "general computing" (Ex. 2026 at 65:9-19), or whether the field of DRM is subsumed within the field of "electronic data protection and distribution." (*Id.* at 78:3-15.) Dr. Madisetti was generally unwilling to answer any questions at his deposition about the basis for his opinions that did not expressly appear in his declaration. *Id.* at 262:22-263:11.

[2] Dr. Madisetti believes the references he cites in his declaration's "Technical Background and State of the Art" section are typical and representative of the references that are familiar to one of ordinary skill in the art in the field of endeavor of the '815 patent." Ex. 2026 at 54:3-16; 56:4-18. Dr. Jakobsson shows that this assertion is false. Ex. 2027 at ¶¶63-75.

customary meaning of such claim as understood by" a POSITA and in view of the intrinsic evidence. 37 C.F.R. § 42.100(b). Petitioner does not propose any terms for construction. Petition at 18-19. Patent Owner agrees that each term may be understood by a POSITA in accordance with its ordinary and customary meaning.

V. STANDARD OF REVIEW

"There is a significant difference between a petitioner's burden to establish a 'reasonable likelihood of success' at institution, and actually proving invalidity by a preponderance of the evidence at trial." *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016); *see also* 35 U.S.C. § 314(a); 35 U.S.C. § 316(e). Because, at the institution phase, the "Board is considering the matter preliminarily [and] without the benefit of a full record," "the Board is not bound by any findings made in its Institution Decision." *Trivascular*, 812 F.3d at 1068. Findings made during Trial are rendered "under a qualitatively different standard" than is used when considering institution. *Id*.; *see also Samsung Elecs. Co., Ltd. v. Infobridge Pte. Ltd*., IPR2017-00100 (Paper 30), at 15 (PTAB Apr. 23, 2018) ("[W]e consider anew [the] arguments presented in [the] Response . . . . We are not persuaded by [the] argument that [PO] has not presented anything new to rebut our previous analysis and conclusion because we now must evaluate the evidence of record against a different, and higher, standard." (internal quotation marks omitted)).

VI. THE PETITION FAILS TO PROVE HANNA IS PRIOR ART

Hanna is an international application filed under the PCT on February 4, 1999. Petitioner alleges that Hanna is prior art under 35 U.S.C. §102(a) as of its August 12, 1999 publication date.[3] *See* Petition at 7-8. The '815 patent was filed on June 7, 2000 and claims priority to the '171 Application, filed on June 8, 1999. *See supra* Section I.B. Since the '815 patent's June 8, 1999 priority date vis-à-vis the '171 Application antedates Hanna's August 12, 1999 publication date, Hanna is not prior art to the '815 patent and Ground 1 should be denied.

A. The '171 Application Provides Adequate Written Description Support for Claims 42 and 43 of the '815 Patent

For a non-provisional patent application to be entitled to the priority date of a provisional application, the latter must "contain a written description of the invention and the manner and process of making and using it, in such full, clear, concise, and exact terms…to enable an ordinarily skilled artisan to practice the invention claimed in the non-provisional application." *Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (internal quotations marks, citations, and emphasis omitted). This written description requirement is satisfied if the disclosure of the provisional application "reasonably conveys to those skilled in

[3] Since Hanna was filed before Nov. 29, 2000, it is not prior art under 35 U.S.C. §102(e). *See* MPEP §2136.03 (9th ed. Rev. Oct. 2019).

the art that the inventor had possession of the claimed subject matter as of the filing date." *In re Global IP Holdings, LLC*, 927 F.3d 1373, 1377 (Fed. Cir. 2019) (internal quotations marks and citations omitted). "This test involves an inquiry into the four corners of the specification from the perspective of a person of ordinary skill." *Id.* The statutory presumption of validity places the initial burden of production and the ultimate burden of persuasion on the party asserting non-compliance with the written description requirement (*e.g.*, Petitioner). *See Ralston Purina Co. v. Far-Mar-Co, Inc.*, 772 F.2d 1570, 1574 (Fed. Cir. 1985).

Compliance with the written description requirement does not require using the identical terms in the specification as used in the claims. Instead, the written description in the specification need only convey to a POSITA a description of what is claimed. *See Inphi Corp. v. Netlist, Inc.*, 805 F.3d 1350, 1354-55 (Fed. Cir. 2015) ("Substantial evidence supports a finding that the specification satisfies the written description requirement when 'the essence of the original disclosure' conveys the necessary information—'regardless of *how* it' conveys such information, and regardless of whether the disclosure's 'words [a]re open to different interpretation[s].'") (internal citations omitted); *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1345-47 (Fed. Cir. 2016) (holding that the overall description of the invention and the patent figures were sufficient to describe the terms even though the claim terms were not used in the specification). Both a patent's specification and

its *drawings* should be considered for what they reasonably convey to a POSITA. *Autogiro Co. of America v. U.S.*, 384 F.2d 391, 398 (Cl. Ct. 1967) ("In those instances where a visual representation can flesh out words, drawings may be used in the same manner and with the same limitations as the specification.") "[D]rawings alone *may* be sufficient to provide the written description of the invention." *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1564 (Fed. Cir. 1991).

Petitioner incorrectly contends that the '171 Application fails to provide written description support for two limitations of Claim 42: Limitation 42[b] ("retrieving at least one digital signature and at least one check value associated with the file") and Limitation 42[c] ("verifying the authenticity of the at least one check value using the digital signature"). Petition at 13-14.[4] As explained below, the '171 Application reasonably conveys to those skilled in the art that the inventors had possession of the claimed subject matter.

Petitioner's priority argument relies entirely on a single fact: that the '171 Application does not include FIGS. 13 and 14 of the '815 patent. *See* Petition at 15. This fact, while true, is insufficient to satisfy Petitioner's burden of proof. The proper written description analysis for Limitations 42[b] and 42[c] requires a close

[4] Petitioner does not provide any evidence or arguments that limitations other than 42[b] and 42[c] found in Claim 42 (or any limitations of Claim 43) allegedly lack adequate written description support. *See* Petition at 13-18.

review of the *entire* comprehensive disclosure of the '171 Application —consisting of 23 pages and 12 drawing sheets—to determine whether the '171 Application "allows persons of ordinary skill to recognize that the inventor 'invented what is claimed.'" *In re Global*, 927 F.3d at 1377 (quoting *Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc).

That is not what Petitioner did. Instead, Petitioner cursorily concludes that FIG. 6 in the '171 Application and its related text in the specification "does not involve retrieving a check/hash value associated with a file, or verifying the authenticity of the check/hash value using the digital signature." Petition at 17. Yet, as described below, FIG. 6 and the corresponding text, along with other portions of the specification and figures such as FIGS. 2D and 3, reasonably convey to a POSITA that the inventor was in possession of the claimed invention. Ex. 2027 at ¶107.

An appropriate review of the '171 Application disclosure begins with FIG. 2D of the '171 Application. Annotated FIG. 2D (below) illustrates "an embodiment of the present invention that solves [the] problems [of the conventional signature encoding techniques shown in FIGS. 2A-2C] by **embedding a block's signature in the watermark of the block that follows the block to which the signature corresponds**." Ex. 1004 at 10-12, FIGS. 2A-2D (emphasis added); Ex. 2027, ¶108. Thus, given a stream of data (*e.g.*, data blocks "n," "n+1," "n+2," etc. at the top of

FIG. 2D), a signature of data block "n" (circled in red) can be embedded into the watermark of data block "n+1" (circled in blue). Similarly, a signature of data block "n+1" (circled in green) can be embedded into the watermark of the following block in the transmission, data block "n+2," and so on. *See* Ex. 1004 at 12-13, FIGS. 2D, 3; Ex. 2027 at ¶109.

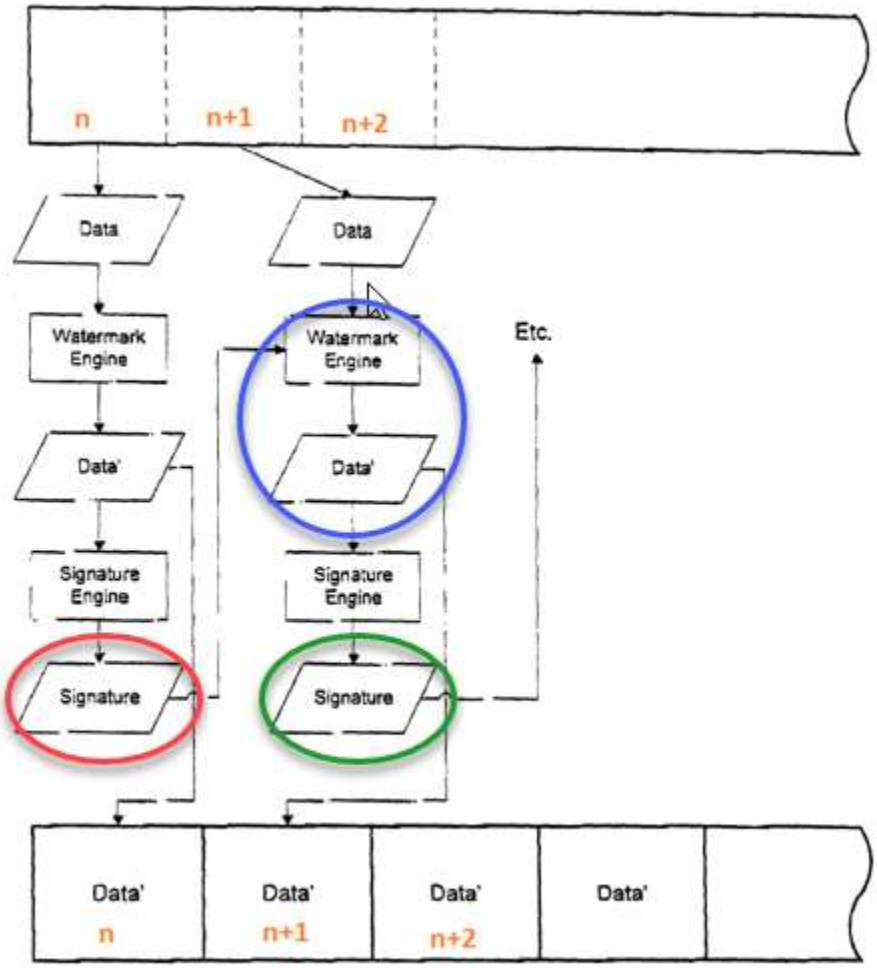

FIG. 2D

The '171 Application explains that a "technological constraint…is that watermarking algorithm[s] typically cannot transport relatively large amounts of

data," and that some of the embodiments described in the '171 Application (*e.g.*, with respect to FIG. 5B and associated text) may use a watermark that contains almost 261 bytes, "which with current technology is a relatively large amount of data for a watermarking algorithm." Ex. 1004 at 20; *see also id.* at 17-19; FIG. 5B; Ex. 2027 at ¶110.

This problem is addressed "through the use of an error-recoverable shared signature scheme" that "is resistant to errors in the signed data," shown and described in the '171 Application with respect to FIG. 6. Ex. 1004 at 20; FIG. 6; Ex. 2027 at ¶111. Annotated FIG. 6 (below) illustrates a process of generating a signed hash concatenation by "first partition[ing]" "a signed data stream 602" (the "Watermark Bloc" shown in blue), and then "hashing apart those partitions and concatenating the resulting hashes." Ex. 1004 at 20, FIG. 6; Ex. 2027 at ¶112. The hash concatenation is next signed. *Id.* FIG. 6 discloses that the signed hash concatenation (colored green) "is contained in the *following* watermarking bloc[k]." Ex. 1004 at FIG. 6 (quoted text in yellow, emphasis added). That is, consistent with the invention described with respect to FIGS. 2D and 3, FIG. 6 teaches that a signature (*i.e.*, the signed hash concatenation) associated with a first data block (*e.g.*, data block "n" in annotated FIG. 2D above) is embedded in the watermark of the following data block (*e.g.*, data block "n+1") in the transmission. Ex. 2027 at ¶113.

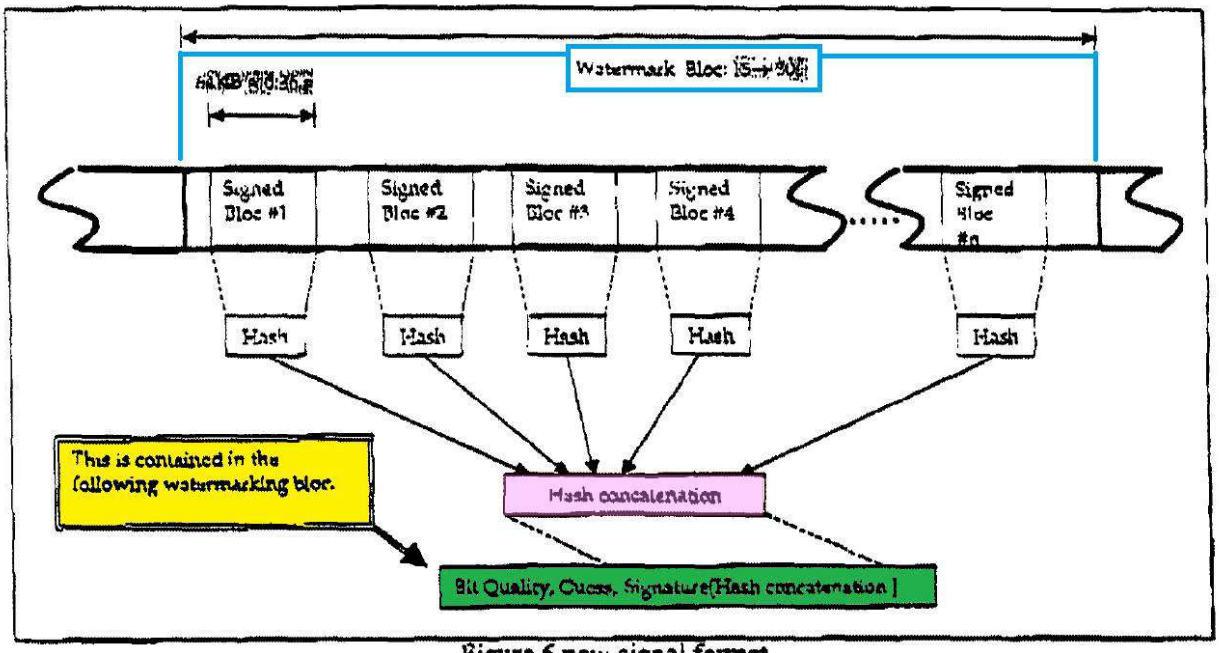

Figure 6 new signal format.

In the "error-recoverable shared signature scheme" disclosed, "**[i]f an error appears on the data, the signature will verify for all partitions except for the one that is affected**." Ex. 1004 at 20 (emphasis added). In this fashion, the '171 Application teaches that such errors "can be readily detected and recovered from." *Id.*; *see also id.* at 6 ("The data signal is divided into a sequence of blocks, and digital signatures of the blocks are embedded in the blocks using watermarks. Ex. 2027 at ¶114. When a user plays or uses the data sequence, the sequence is checked for the presence of the watermark containing the digital signature. **If this watermark is found, then the digital signature is used to verify the authenticity of the content**.") (emphasis added); *Id.*. Thus, the digital signature received in the

watermark of the following data block (*e.g.*, data block "n+1") is used to verify the preceding data block (*e.g.*, data block "n"). *Id.*

To that end, the disclosure of the *entire* '171 Application would reasonably convey to a POSITA that the claimed "digital signature" would first be extracted from the watermark of the successive data block (*e.g.*, data block "n+1") to proceed with verification of the "current" data block (*e.g.*, data block "n") (*e.g.*, teaching, in part, Limitation 42[b]: "retrieving at least one digital signature…associated with the file"). Ex. 2027 at ¶115. The signature would then be, for example, "decrypted" using the public key of the signer to reveal the "unencrypted" hash concatenation to be used for comparison matching with the hash concatenation of the "current" data block.[5] *Id*. As part of the verification process, a POSITA would understand that the hash concatenation of the current data block would be retrieved (*e.g.*, from received data block "n") by partitioning and hashing the current data block (*e.g.*, disclosing, in part, Limitation 42[b]: "retrieving…at least one check value associated with the file").[6] Ex. 2027 at ¶116. A comparison can then be made between the hash

[5] Digital signature verification does not necessarily entail "decryption," but since the '171 Application expressly discloses the use of the RSA algorithm (*see* Ex. 1004 at 19), a POSITA would understand that decryption may be used as part of the verification process.

[6] A POSITA would also understand that the watermark of the current data block would be another form of "check value" that would also be retrieved. Ex. 2027 at ¶¶120-122.

concatenation retrieved from the current data block and the hash concatenation extracted from the digital signature in the watermark of the successive data block (*e.g.*, data block "n+1"). *See* Ex. 1004 at 20 ("If an error appears on the data, the signature will verify for all partitions except for the one that is affected."); *see also id.* at FIG. 2C (illustrating signature verification by comparing a hash of the data block received (*i.e.*, " X ") and a hash of the unsigned signature (*i.e.* " X' ")); Ex. 2027 at ¶117. When the hash concatenation extracted from the digital signature is compared to the concatenation of hash values retrieved from the received data block, a match between the two (or parts thereof[7]) verifies the authenticity of the hash concatenation retrieved from the received data block (*e.g.*, claimed "check value") (*e.g.*, disclosing Limitation 42[c]: "verifying the authenticity of the at least one check value using the digital signature").Ex. 2027 at ¶118. The individual hashes that make up the concatenation of hash values can then be used, one by one, to verify the authenticity of corresponding partitions of the data block received (*e.g.*, disclosing Limitation 42[d]: "verifying the authenticity of at least a portion of the file using the at least one check value"). Ex. 2027 at ¶119.

[7] The entire hash concatenation values do not need to match in their entirety to authenticate the check value since the '171 Application explains that a statistical analysis can be used to determine the "appropriate number of correct blocks" needed "to decide that the signature is correct." Ex. 1004 at 20; Ex. 2027 at ¶118.

Thus, the '171 Application provides written description support for the limitations of claim 42. Ex. 2027 at ¶123. Petitioner's failure to fully analyze the entire disclosure is fatal to its argument. Tellingly, Petitioner incorrectly summarizes the relevant disclosures found in the '171 Application, including FIG. 6 and its related text in the specification, by cursorily concluding that "[l]ike the other embodiments disclosed, the 'shared signature' technique [of FIG. 6] does not involve retrieving a check/hash value associated with a file, or verifying the authenticity of the check/hash value using the digital signature." Petition at 17; Ex. 2027 at ¶107. Yet, as described above, FIG. 6 and the corresponding text, along with other portions of the specification and figures, reasonably convey to a POSITA "retrieving at least one digital signature and at least one check value associated with the file" (Limitation 42[b]) and "verifying the authenticity of the at least one check value using the digital signature" (Limitation 42[c]).

Accordingly, the '171 Application satisfies the written description requirement because "'the essence of the [its] disclosure' conveys the necessary information—'regardless of *how* it' conveys such information" to show that the inventors were in possession of the subject matter recited in claims 42 and 43. *See Inphi Corp.*, 805 F.3d at 1354-55. As in *Autogiro* and *Blue Calypso*, the specification and figures of the '171 Application *together* provide clear support for Limitations 42[b] and 42[c] (and the other limitations of claims 42 and 43 not

challenged by Petitioner). *Autogiro*, 384 F.2d at 398 ("In those instances where a visual representation can flesh out words, drawings may be used in the same manner and with the same limitations as the specification."); *Blue Calypso, LLC*, 815 F.3d at 1345-47. As such, the Challenged Claims are entitled to the priority date afforded by the '171 Application, and Hanna, which was published more than two months after the '171 Application's filing date, is not prior art under 35 U.S.C. §102(a). Ex. 2027 at ¶124. Ground 1 should therefore be denied.

B. Hanna is Not Analogous Art

Even if the Board were to determine that Hanna is prior art to the Challenged Claims, Hanna is not analogous prior art, and therefore cannot provide the basis for an obviousness challenge. "A reference qualifies as prior art for an obviousness determination under §103 only when it is analogous to the claimed invention." *In re Klein,* 647, F.3d 1343, 1348 (Fed. Cir. 2011). "Two criteria have evolved for determining whether prior art is analogous: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved." *In re Clay*, 966 F.2d 656, 658–59 (Fed. Cir. 1992). Under this long-standing test, Hanna is not analogous art, and therefore does not qualify as prior art that can be used to invalidate the Challenged Claims.

First, the Challenged Claims and Hanna are in separate fields. The Challenged Claims are in the field of digital piracy protection and/or DRM. Accordingly, the '815 patent describes its field as generally related to "protecting data from unauthorized use or modification," and specifically to "using digital signature and watermarking techniques to control access to, and use of, digital or electronic data." Ex. 1001 at 1:24-25, 2:46-48. Hanna, on the other hand, is in the field of transmission-related data corruption detection. Ex. 1006 at 3:1-4 (stating that its field of invention "relates to data corruption detection and, more particularly, to a method and apparatus for efficient authentication and integrity checking in data processing using hierarchical hashing.") Petitioner ignores Hanna's description to contend (without evidentiary support beyond its expert's conclusory declaration) that Hanna's field is "electronic data protection and distribution," but as Dr. Jakobsson explains, this classification is unduly broad, inaccurate and unhelpful.[8] Ex. 2027 at ¶¶125-127

One way to understand why the fields of endeavor for the '815 patent and Hanna are different is by considering how each addresses a very different

[8] Indeed, Petitioner's expert has identified DRM as a separate field from "data protection" in a co-pending IPR. *See* Ex. 2024 at ¶¶46, 48. He also purports to have his own issued patents in the field of DRM. Ex. 1002 at ¶28. But at deposition, Dr. Madisetti said he was "not offering a definition of DRM" and was unable to identify any of his patents in that field. Ex. 2026 at 25:2-3, 89:16-92:9.

"adversarial model" (or "threat model"). The adversarial model is a specification of the threat being addressed by a system. Ex. 2027 at ¶53. Adversarial models have been a prominent part of security research since at least the 1980s, and a POSITA would understand that they are important to take into consideration when designing an electronic data system.[9] Ex. 2027 at ¶¶55-58. The adversarial model may be applied to a system in the field of digital piracy protection and/or DRM techniques. *Id*. at ¶¶52, 54. In such a system, the potential adversary of the content owner is the user of the device containing the content. *Id*. at ¶¶52, 54, 83-89. The adversarial model may also be applied to systems in the field of transmission-related data corruption detection. Id. at ¶59. In such a system, the potential adversary is not the receiver of the data transmission because both the sender and receiver are aligned in that they both do not want any of the transmitted data to be corrupted. *Id*. Rather, one potential adversary during data transmission is any of countless, unknown third parties on the network that may corrupt data. Another potential adversary during data transmission is the network itself, which can cause errors during transmission. *Id*.

[9] Dr. Madisetti generally refused to answer questions about the adversarial model because he has "not offered such an opinion in my declaration." *See, e.g.*, Ex. 2026 at 44:4-10. 44:15-20.

Second, because the differences in the applicable adversarial models present very different security threats, a POSITA would consider Hanna and the Challenged Claims as being directed to addressing different problems. *Id*. at ¶¶60-62. The preamble of the Challenged Claims indicate that their purpose is to "manag[e] the use of a file of electronic data." In the context of the '815 patent, the claimed inventions intend to defeat *intentional* attempts to circumvent controls that are designed to prevent unauthorized use by a potential user. On the other hand, Hanna purports to address "a need for a system that protects against *unintentional* data corruption and malicious acts that cause errors in data processing," Ex. 1006 at 3:1-4 (emphasis added); Ex. 1002 at ¶75 (Dr. Madisetti agrees that this is the "objective" of Hanna).; Ex. 2027 at ¶¶ 128-129. In contrast to the '815 patent, Hanna is not addressing malicious interference on the device that *receives* the data. In Hanna, there is not a component running on one device that has a potentially adversarial relationship with another component running on the same device. Hanna describes methods that seek to detect data corruption by an adversary that is on the network, rather than one on the device that is configured to use the data, such as the intended device (and content) user. *See, e.g.,* Ex. 1006, 9:24-26 ("If the signature fails this verification step or it is determined that the packet was corrupted during transmission, the top level packet must be repaired or recovered before checking the other packets (steps 330, 335).") Repairing or recovering data addresses network

corruption, but does nothing to protect against unauthorized use in a predefined manner by an adversary on the same device as the content. Ex. 2027 at ¶134.

For the foregoing reasons, Hanna is not analogous prior art and cannot support an obviousness challenge to the Challenged Claims. Accordingly, Ground 1 should be denied.

VII. THE PETITION FAILS TO PROVE THAT CLAIMS 42 IS INVALID BASED ON HANNA AND STEFIK (GROUND 1)

The Petition alleges that claim 42 is unpatentable as being obvious over Hanna in view of Stefik. However, as explained below, even if Hanna is found to be analogous prior art, the Petition fails to meet its burden of proof for several reasons.

A. Hanna Fails to Disclose Limitation 42[a]

Petitioner's contention that Hanna discloses Limitation 42[a] is wrong. Petitioner points to three disclosures in Hanna as alleged support, but none of these portions discloses "receiving a request to use [a] file in a predefined manner." *See* Petition at 31 (citing Ex. 1006 at 7:16-18, 7:24-26 ("application program"), 1:10-13 (remote back up), 1:13-15 (video conferencing)). Although each of these three operations may involve a request of some sort, there is no basis to assume, as Petitioner does, that those requests indicate a predefined use of the data. As the plain language of the claim demonstrates, Limitation 42[a] cannot be satisfied by a mere generalized request. Moreover, it is undisputed that Hanna does not apply its hierarchical hashing scheme to any of these three operations. Indeed, each is

discussed in Hanna before that scheme is introduced, and they are never mentioned again.

First, Petitioner misleadingly implies that Hanna's discussion concerning an "application program" (at 7:15-26) involves receiving an application program that is cryptographically verified according to Hanna's data processing protocols (*e.g.*, hierarchical hashing scheme). *See* Petition at 26-27 (citing Ex. 1006 at 7:15-23), 31 (citing Ex. 1006 at 7:16-18, 7:24-26). Hanna makes no such disclosure. Ex. 2027 at ¶151. Instead, this portion of Hanna is discussing the initial transmission of the software that will be installed at computer 100 to implement Hanna's hashing scheme. Hanna explains that the "requested [application] code" is transmitted from the remote server 130 (*see* FIG. 1 below) to computer system 100 over the network 122, 126, 128 to "***provide[] the data processing operations described herein***." Ex. 1006 (Hanna) at 7:16-20 (emphasis added); 5:22-28, 6:3-25. Ex. 2027 at ¶152. Hanna does not teach that this software transfer is performed using Hanna's hashing scheme (described in Hanna with respect to FIGS. 2-5), nor could it, since there would be no prior software residing on computer system 100 capable of carrying out Hanna's data processing protocols as computer system 100 receives this software. Ex. 2027 at ¶153. Thus, any "request" for Hanna's hashing scheme application program is irrelevant to the Challenged Claims, which require that the "file"

requested be the subject of the digital signature(s) and check value(s) retrieved and verified. Ex. 1001 at 32:13-29; Ex. 2027 at ¶154.

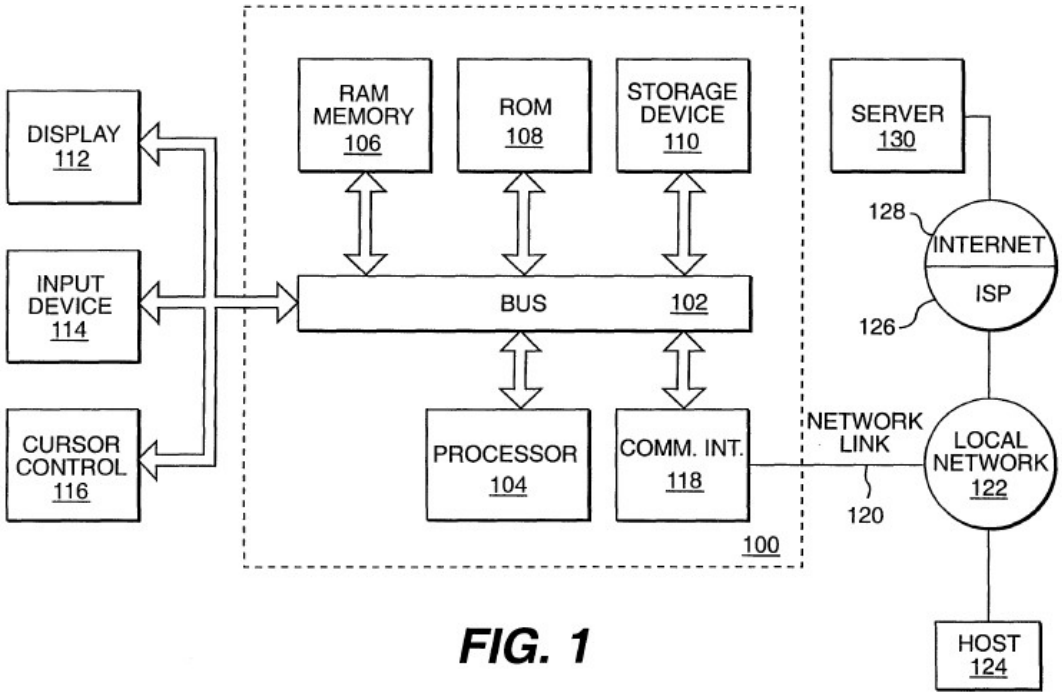

FIG. 1

Second, attempting to fill in the gaps in Hanna's disclosure, Petitioner makes an *inherency* argument, asserting that, for both computer file backups and video conferencing, a POSITA would inherently understand that requests to use the files in a predefined manner would "***necessarily***" be present in Hanna. *See* Petition at 28 (emphasis added); *see also id.* at 31 ("A POSITA would recognize that in each case a request to transmit, copy and/or store files of electronic data ***is made***.") (emphasis added). However, inherency requires "that the limitation at issue necessarily must be present"—"mere possibility is not enough." *PAR Pharm., Inc. v. TWI Pharm.,*

Inc., 773 F.3d 1186, 1195-96 (Fed. Cir. 2014); *Personal Web Techs., LLC v. Apple, Inc.*, 917 F.3d 1376, 1382-83 (Fed. Cir. 2019).

Receiving a request to use a file in a predefined manner is anything but "necessarily present" in Hanna's teachings. In support of its inherency argument, Petitioner relies on two disclosures in the "Description of Related Art" section that describe prior art systems relating to "business activities" that "create the need to transfer information in a secure manner." Ex. 1006 at 1:10-11. Hanna's lone sentence concerning backing up files states that banks "periodically 'backup' files to a remote central server," but it provides no disclosure that this "backup" is performed in response to a request to use the files in a predefined manner, let alone that it is performed using Hanna's hierarchical hashing scheme. *See* Ex. 1006 at 1:11-13; Ex. 2027 at ¶ 156. Petitioner speculates the that requested predefined use *could* be "to transmit, copy and/or store" data. But Petitioner does not provide any basis in Hanna for why a bank would send a request that needs to be granted (by whom?) before it can "transmit, copy and/or store" its own data. Indeed, Hanna teaches that any transmission, copying and/or storing of such data would begin before the entire file is received. *See* Ex. 1006 at 8:10-11 ("Systems consistent with the present invention generally begin the hashing process by dividing the data set into small packets (step 210)"; 12:4-5 ("Systems consistent with the present invention need not wait for all of the packets to be delivered to verify a data packet."); Ex. 2027 at ¶ 157.

Nor is a bank backing up its own data a "predefined use" that is covered by the Challenged Claims. The '815 patent is concerned with "attackers" transmitting perfect, but unauthorized, copies of content to others, or removing data related to the content placed there to restrict the attacker's use. *See*, *e.g.*, *id.* 9:27-29 ("it is desirable to prevent ***attackers*** from copying a digital file from a storage medium such as a compact disc and ***distributing unauthorized copies to others***."); 9:32-36 ("***attackers*** often employ compression techniques to reduce content files to a fraction of their original size, thus ***enabling copies to be transmitted*** over networks such as the Internet with relative ease"); 9:52-57 (if a content file contains special codes indicating…that the content cannot be compressed, copied, or transmitted, ***an attacker may attempt to remove those codes*** in order to make unauthorized use of the content.") (emphases added). Because a bank is not at risk of "attacking" its own data, the requesting (and granting) steps recited in the Challenged Claims are not practiced in this backup example. Ex. 2027 at ¶¶158-160.

Hanna also does not disclose that prior art "video conferencing" involves the receipt of a request to a use a file in a predefined manner (including providing no information about which of the video conferencing participants would receive such a request, what "file" would be used, and in what predefined manner), or how its

hashing scheme would apply (if at all) to this application. Ex. 1006 at 1:13-15.[10] Ex. 2027 at ¶161. A POSITA would understand that a video conference involves a *real time* transmission of a data stream, and does not implicate a "request to use [a] file in a predefined manner." Ex. 2027 at ¶162. For example, when one party initiates the video conference, there is no "file" to request (or even in existence) to use in "a predefined manner." Petitioner's expert, Dr. Madisetti, conceded that at the outset of the video conference there would be no file to request to use in any manner, just "bandwidth capabilities, the codecs, and specification of the codecs being used." Ex. 2026 at 12:17. Moreover, none of the participants are potential "attackers" who would need to make a request to use a file in a predefined manner to participate in the video conference. Ex. 2027 at ¶162.

Accordingly, Petitioner's inherency argument fails because "receiving a request to use [a] file in a predefined manner" is not an inevitable, necessary consequence to using Hanna's data processing protocols for periodic bank backups or video conferencing. Ex. 2027 at ¶164. For the reasons above, Hanna does not teach or disclose Limitation 42[a] "receiving a request to use the file in a predefined manner."

[10] Indeed, the word "request" appears nowhere in Hanna except in relation to the "requested code for an application program." *See* Ex. 1006 at 7:17; Ex. 2027 at ¶163.

B. Hanna Fails to Disclose Limitation 42[e]

There is no dispute that Hanna does not expressly teach or disclose "granting the request to use the file in the predefined manner." Petitioner nevertheless suggests that Hanna inherently teaches the "granting" step because it discloses that data portions that are not verified "should be repaired, recovered, or discarded." Petition at 38. According to Petitioner, "[a] POSITA would have recognized that corrupted data, or data not properly signed with a recognized/authenticated signature, would be undesirable to be used." *Id.*; Ex. 2027 at ¶166. But Hanna's hierarchical hashing scheme requires that each file is divided into a set of portions, and teaches that portions of the data may be verified even "if other portions of the data are corrupt or have not yet been received." Ex. 1006, at 3:10-17. Ex. 2027 at ¶167. Thus, Petitioner's contention that "it would have been obvious to allow or prevent a requested use of a file depending on whether it passes the authentication process" (Petition at 38) makes no sense because some portions of the file may be verified while others are not. *Id*.

For example, in Hanna's prior art backup application, a POSITA would understand that a user would not accept a partially corrupted file. *See* Ex. 1006, 1:21-13 (banks "need to know that these files were successfully copied to the remote database without having been changed or corrupted during the process"); Ex. 2027 at ¶168. Moreover, Petitioner concedes that a POSITA would understand that Hanna

is intended to benefit the user, rather than to prevent the user's unauthorized use of the data, as is required by claims 42 and 43. *See* Petition at 9 ("A POSITA would have recognized that corrupted data…would be undesirable to be used.") Indeed, repairing or recovering data addresses network corruption during transmission, but does nothing to protect against an adversarial user (i.e., *an attacker*) that is on the same device as, and has potential access, to the content. Ex. 2027 at ¶169. That is because Hanna's focus is on securing the transmission of data, not how the data is processed or used by an application on the device after it is received. Unlike the '815 patent, Hanna is agnostic when it comes to how received data is eventually consumed at the device. Ex. 2027 at ¶168.

Because Petitioner fails to show that the "granting" step is necessarily present in Hanna, Hanna inherently does not teach or disclose Limitation 42[e]. Ex. 2027 at ¶170.

C. A POSITA Would Not Have Been Motivated to Combine Hanna and Stefik to Achieve a Combination That Discloses Limitations 42[a] and 42[e]

As shown above, Hanna does not disclose multiple limitations of the Challenged Claims. Petitioner does not allege that a POSITA would modify Hanna's teachings, which relate to a different field and purport to solve very different problems than the Challenged Claims, to add the "receiving" and "granting" steps. Rather, Petitioner asserts that it a POSITA would have been motivated to modify

Hanna with Stefik to "allow or prevent a requested use of a file depending on whether it passes the authentication process." Petition at 38. Petitioner's argument that a POSITA would incorporate Stefik's *granting* of a request to use the file in a predefined manner *presumes* that Hanna teaches that its system receives such a file request in the first place. As shown above, Hanna does not disclose the recited request to use a file in a predefined manner. A POSITA would not have been motivated to make the asserted modification of adding Stefik to grant a non-existent request.

Petitioner argues that even if Hanna does not disclose "receiving a request to use the file in a predefined manner" and "granting the request to use the file in the predefined manner," Stefik allegedly teaches these limitations (though no others). Petition at 31-33, 38-39; *see also id.* at 28. But assuming, *arguendo,* that Stefik discloses the "receiving a request…" and "granting the request…" steps of the Challenged Claims, Petitioner fails to show that a POSITA would have been motivated to combine and modify Hanna with the teachings of Stefik to achieve a combination having the claimed features. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1367-68 (Fed. Cir. 2016) (an obviousness determination requires finding *both* "that a skilled artisan would have been motivated to combine the teachings of the prior art…and that the skilled artisan

would have had a reasonable expectation of success in doing so."); *see also In re Stepan Company*, 868 F.3d 1342, 1346 (Fed. Cir. 2017) (same).

In an attempt to purportedly show that a POSITA would have been motivated to modify Hanna in view of Stefik, Petitioner proffers a number of reasons why Hanna and Stefik are allegedly similar. *See* Petition at 28-29 (both systems include computer equipment "remote from each other;" "same field of endeavor (digital file security);" address same problem of "unauthorized manipulation of digital files;" both use signatures, certificates, and hash functions). But, as shown below, these alleged similarities would not have motivated a POSITA to combine two dissimilar references.

As an initial matter, Hanna and Stefik are *not* directed to the same field of endeavor. Ex. 2027 at ¶174. Petitioner contends that "both references are from the same field of endeavor (digital file security)." Petition at 29. Petitioner provides no description of the purported field of "digital file security," but Dr. Madisetti testified that it has the same meaning as the field of "electronic content protection and distribution" that Petitioner improperly attributes to the '815 patent. Ex. 2026 at 171:16-172:1; Ex. 2027 at ¶¶42-45. Nevertheless, the evidence does not support that Hanna and Stefik are in the same field. As discussed above, Hanna discloses that it is directed to the field of transmission-related data corruption detection. By contrast, Stefik's field of endeavor is not data corruption detection, but piracy protection

and/or DRM.[11] *See* Ex. 1007 at 1:5-8 ("relates to the field of distribution and usage rights enforcement for digitally encoded works"); Petition at 23 (acknowledging that Stefik is "directed to a method and system for controlling usage and distribution of digital works, such as software."); Ex. 2027 at ¶174.

Petitioner is also incorrect that "both references…address the problem of unauthorized manipulation of digital files." Petition at 29; Ex. 2027 at ¶175. Although Hanna expressly states that it addresses the problem of "unintentional data corruption and malicious acts that cause errors in data processing" (Ex. 1006 at 3:1-4), Stefik addresses a very different problem. Ex. 2027 at ¶175. Petitioner concedes that Stefik "recognizes the problem of unauthorized distribution and usage of digital work," and provides no evidence from the patent to support its contention that it also deals with the problem of unauthorized manipulation of digital files. Petition at 23. Stefik says that a "major concern" is preventing an unauthorized user from being able to "'perfectly' reproduce[] and distribute[]" the digital work, not preventing an unauthorized modification of the work during transmission. *Id.* at 1:10-28.

Hanna and Stefik's also propose significantly different solutions to their respective problems. Ex. 2027 at ¶176. Hanna divides a data set into portions, and

[11] Dr. Madisetti testified that "I don't have an opinion one way or the other" about whether Stefik is in the field of DRM because "that's not something I've considered as a part of my first declaration." Ex. 2026 at 82:11-17.

then "create[s] a hierarchy of hash values" that "allows a single digital signature to protect the data set from both data corruption and malicious acts that cause errors in data processing." *Id.* at 3:6-8. "Receiving this hierarchy of hashes before the data also allows the data packets to be quickly verified as they are received." *Id.* at 3:8-10. Conversely, Stefik does not teach dividing a work into small portions, and applying a hash function to each of them. Ex. 2027 at ¶176. Rather, Stefik teaches that a "key feature of the present invention" is permanently attaching usage rights to the entire work, not splitting the work up. *Id.* at 6:51-56; 3:50-58 (providing a system where the "owner of a digital work [] attach[es] usage rights to the work" that "define how it may be used and distributed"). Stefik explains that "'usage rights'…is a term which refers to rights granted to a recipient of a digital work." *Id*. at 6:43-45. "[T]hese rights define how a digital work can be used and if it can be further distributed," and each "may have one or more specified conditions which must be satisfied before the right may be exercised." *Id*. at 6:45-50. A POSITA would, therefore, not look to Stefik's digital works distribution and usage rights system that leverages a "means for billing [that] is always transported with the work," (*id*. at 3:46-48), to modify Hanna's transmission-related data corruption detection system (including its hierarchical hashing scheme) because Hanna has nothing to do with the enforcement of usage rights. Ex. 2027 at ¶176. Accordingly, because Hanna and Stefik are in different fields and address different problems in significantly

different ways, a POSITA would not have been motivated to look to Stefik to modify Hanna's teachings. *Id.*

Moreover, Petitioner's grossly simplistic and unsupported analysis that a POSITA would have been motivated to combine these two references because they both describe "remote" computer systems and use basic, ubiquitous cryptographic functions (such as digital signatures, certificates, and hashes) serves nothing more than to obfuscate how different these references are, both in terms of *what* they set out to accomplish and *how* they do it. These superficial similarities fail to explain why a POSITA would have been motivated to *modify* Hanna's system to incorporate the teachings of Stefik. Petition at 28-30. Prior art can only be combined to invalidate a claim if there is, in fact, a reason for a POSITA to have done so at the time of the invention. *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1360 (Fed. Cir. 2012) ("motivation must be shown" to combine prior art to invalidate a claim).

The ***only*** reason Petitioner provides for why a POSITA would have been motivated to modify Hanna in view of Stefik is because "it would facilitate timely detection of data corruption in a file of electronic data, *i.e.*, when data that could be corrupted or hacked during transmission is about to be used." Petition at 29. However, Hanna's system already provides for timely detection of data corruption through its hierarchical hashing scheme that "allows [] data packets to be quickly

verified as they are received." Ex. 1006 at 3:8-10; *see also id.* at 3:2-3, 12:3-10, 12:17-21; Ex. 2027 at ¶177. Moreover, Hanna already ensures that corrupted data is not delivered to the intended recipient, let alone used, because any corrupt packet "must be repaired or replaced before any packets that depend on this hash block can be verified." Ex. 1006 at 10:9-11; Ex. 2027 at ¶177. Since Hanna's system detects data corruption concurrently with its transmission, modifying Hanna's data corruption detection scheme as Petitioner proposes to include "receiving a request…" and "granting the request…" would not provide any meaningful improvement in Hanna's detection time. Ex. 2027 at ¶176.

Because Petitioner has failed to meet is burden to show how and why a POSITA would have been motivated to modify Hanna's transmission-related data corruption detection scheme that uses hierarchical hashing with Stefik's digital works usage rights system to achieve a combination that includes the Challenged Claims' "receiving a request to use [a] file in a predefined manner" and "granting the request…." steps, Ground 1 should be denied. *Id*.

VIII. THE PETITION FAILS TO PROVE THAT CLAIM 42 IS INVALID BASED ON GENNARO ALONE (GROUND 2)

The Petition alleges that claim 42 is unpatentable as being obvious over Gennaro by itself. However, as explained below, the Petition fails to meet its burden of proof for several reasons.

A. Gennaro is Not Analogous Art

Gennaro may not be considered for an obviousness determination under § 103 because, like Hanna, it is not analogous to the claimed inventions. *See In re Klein,* 647 F.3d 1343, at 1348.

As demonstrated above, the Challenged Claims are in the field of piracy protection and/or DRM. Gennaro is in the same field of endeavor as Hanna; namely, transmission-related data corruption. Gennaro describes its technical field as a "“method of signing and authenticating a stream of data using a reduced number of digital signatures.” method of signing digital streams so that a receiver of the stream can authenticate and consume the stream at the same rate which the stream is being sent to the receiver." Ex. 1008 at 1:4-6; Abstract ("A method of signing digital streams so that a receiver of the stream can authenticate and consume the stream at the same rate which the stream is being sent to the receiver.") As explained by Dr. Jakobsson, authenticating transmitted data streams (*i.e.,* detecting whether the stream has been corrupted during transmission) is in a different field of digital security than that of the '815 patent, which protects data from unauthorized use by the recipient, because they are associated with different adversarial models. Ex. 2027 at ¶142.

Gennaro and the Challenged Claims are also directed to addressing different problems. Unlike the '815 patent, Gennaro is not concerned with defending the

streamed content against an attacker that is present on the device receiving the content and intent on accessing and using the content in an unauthorized manner. *Id*. Indeed, Gennaro is not concerned with how content will be used by the recipient at all. *Id*. This view is consistent with the fact that Gennaro discloses neither an anti-piracy nor DRM system, instead purporting to address problems presented by prior art stream signing methods that "resort to storing large portions of the data stream" and "maintaining excessively large authentication tables." Ex. 1008 at 2:32-35; Ex. 2027 at ¶142. Gennaro seeks, as does Hanna, "to reduce computation time necessary to sign and authenticate a stream of data by reducing the number of digital signatures required for one to authenticate the data stream," thereby allowing the receiver to "consume authenticated data from the stream at the same rate he receives such data from the stream." Ex. 1008 at 2:29-32, 2:35-41; 14:13-16 ("when [u]sing our solution [to transmit log files,] the receiver can interrupt the transmission as soon as tampering is detected thus saving precious communication resources."); Ex. 2027 at ¶¶143-144. In other words, while the '815 manages the use of content by ensuring it is not used in an unauthorized way, Gennaro is focused on the unrelated issue of facilitating delivery of uncorrupted content to the user and preserving network resources. Because Gennaro is not analogous art to the '815 patent, Ground 2 should be denied.

B. Gennaro Fails to Disclose Limitation 42[a]

Ground 2 should also be denied because Gennaro does not disclose multiple limitations of the Challenged Claims. Petitioner provides a number of misleading arguments in its attempt to show that Gennaro discloses Limitation 42[a]: "receiving a request to use the file in a predefined manner." As explained below, all of these contentions fail to support Petitioner's assertion.

"In appropriate circumstances, a single prior art reference can render a claim obvious. However, there must be a showing of a suggestion or motivation to modify the teachings of that reference to the claimed invention in order to support the obviousness conclusion." *SIBIA Neurosciences, Inc. v. Cadus Pharm. Corp.,* 225 F.3d 1349, 1356 (Fed. Cir. 2000). Neither Petitioner nor its expert have identified any such suggestion or motivation for a skilled artisan to modify Gennaro to arrive at the inventions of the Challenged Claims.

First, Petitioner contends, without support, that Gennaro "discloses" that a "sender receives [a] ***'request'*** from the receiver." Petition at 48. Gennaro makes no such disclosure. Indeed, the word "request" is used one time in Gennaro, and in a very different context related to accommodating classes and data resources. *See* Ex. 1008 at 13:35-46; Ex. 2027 at ¶181.

Second, Petitioner incorrectly asserts that "Gennaro discloses ***a user requesting*** to use a file in a predefined manner (e.g., playing 'internet applications

(digital movies, digital sounds, applets)')." Petition at 49 (citing Ex. 1008 at 2:64-67). Ex. 2027 at ¶182. What the cited section of Gennaro actually discloses is that "digital movies, digital sounds, [and] applets" are finite streams that are known in their "entirety to the signer in advance." Ex. 1008 at 2:64-3:4; Ex. 2027 at ¶182. These streams are divided into blocks, and Gennaro asserts "a single hash computation will suffice to authenticate the [] blocks." Ex. 1008 at 2:55-57, 2:67-3:2; Ex. 2027 at ¶183. Gennaro does not teach or disclose anything in this section regarding how the recipient may use the authenticated stream (if, in fact, it actually receives the stream)[12], including any suggestion that this process is initiated by receiving a request to use these "digital movies, digital sounds, [and] applets" in a predefined manner. Ex. 2027 at ¶183. And, contrary to Petitioner's expert's statement, Gennaro also does not disclose "*rendering* or *playing*" these internet applications. *See id.*; Ex. 1002 at ¶140; Ex. 2027 at ¶184. Thus, Petitioner's expert's subsequent conclusion that a "POSITA would have understood ***such [rendering or playing]*** as a user requesting to use a file in a predefined manner (*e.g.*, ***play***)" is unfounded and unsupported by the evidence. Ex. 1002 at ¶140; Ex. 2027 at ¶184. In any event, it is undisputed that Gennaro does not apply its method of signing and

[12] If a block is determined to be corrupted, "then tampering has been detected and processing halted." Ex. 1008 at 5:57-58; Ex. 2027 at ¶183. Moreover, the MPEG software on the receiving device is not even made aware of this corrupted data block. *Id*. at 5:36-38; Ex. 2027 at ¶183.

authenticating a data stream to manage a user's "rendering or playing" of that data stream.

Third, Petitioner misleadingly argues that Gennaro (at 1:28-29) "discloses that, when a user requests to play a file, a receiver requests transmission of the digital stream comprising the video for that purpose." Petition at 49. But Gennaro makes no such disclosure. Ex. 2027 at ¶185. Rather, Gennaro describes a prior art system[13] where a "receiver asks for [an] authenticated stream." Ex. 1008 at 1:23-33. Asking for an authenticated stream of data is not the same thing as "receiving a request to *use [a] file in a predefined way*" because asking for data is not a request to use that data in any particular way. Ex. 2027 at ¶186. Indeed, as Gennaro discloses, data may not be used until it is first authenticated. *See* Ex. 1008 at 5:8-12. Accordingly, it is of no moment whether "a POSITA would make similar requests [for authentication] for *all file transmissions*" (Petition at 49) (emphasis added) because authentication is a prerequisite for any use. *See*, *e.g.*, Ex. 1008 at 5:36-39 ("the MPEG software that may play the stream is not informed of incoming data before it is authenticated" to prevent it from "consuming unauthenticated data.") There is no

[13] The cited portion (Ex. 1008 at 1:28-29) relates to the description of a *prior art system*—one that Gennaro identifies as having a "problem." *See* Ex. 1008 at 1:7, 1:23-36; Ex. 2027 at ¶185. Petitioner provides no evidentiary basis to explain why a POSITA would be motivated to use prior art that has been expressly criticized by Gennaro to modify Gennaro's own teachings.

suggestion or motivation within Gennaro that the user should then make a ***second request*** to use any authenticated data "in a predefined manner."

Finally, Gennaro explains that its system "requires additional authentication software to be added to any existing MPEG software or hardware." Ex. 1008 at 5:4-6; Ex. 2027 at ¶187. The authentication software authenticates the incoming data blocks before passing them on to the MPEG software that converts the received blocks back into video. *Id.* at 5:7-11; Ex. 2027 at ¶187. This authentication software is tasked with informing the MPEG software of incoming data that has been authenticated. *Id.* at 5:15-20, 5:35-39; Ex. 2027 at ¶187. Petitioner contends that it would have been obvious to a POSITA "to configure" the receiver in Gennaro "so that, when it passes the data to the authentication software, it is in the context of a request for the MPEG software to convert the data into video for playback." Petition at 49. But Petitioner fails to explain what specifically about the addition of the authentication software to the front-end of a standard MPEG receiver would suddenly inspire a POSITA to "configure" the receiving system to operate in the context of receiving *a request to use a file in a predefined manner*. Ex. 2027 at ¶188. When asked to explain why a POSITA would configure the receiver to send "a request for the MPEG software to convert the data into video for playback," Dr. Madisetti first said "There's no request to the MPEG software." Ex. 2026 at 260:9-14. After realizing that this testimony was inconsistent with his declaration (Ex.

1002 at ¶142), he said a POSITA could make another modification so that the "MPEG software itself could request for authorization." *Id*. at 260:16-261:5. Once it was pointed out that the MPEG software is unaware of a block until *after* it is authorized, he said that the "receiver could make the MPEG software aware to the extent that the MPEG software needs to be modified." *Id*. at 261:3-12. Dr. Madisetti's convoluted testimony, which adds at least two further modifications that a POSITA would need to make to Gennaro that were not provided in either the Petition or his declaration, conclusively demonstrates that the required changes would be anything but obvious.

In place of providing a cogent explanation, Petitioner puts forth a conclusory argument: because the authentication software passes authenticated data (but not inauthentic data) to the MPEG software, it necessarily would be in response to a request to use a file in a predefined way. *See* Petition at 49. The Federal Circuit has consistently held that a Petitioner cannot rely on conclusory statements to satisfy its obviousness burden. Petitioner has failed to make the requisite "showing of a suggestion or motivation to modify the teachings of that reference to the claimed invention." *SIBIA,* 225 F.3d at 1356. At best, Petitioner's conclusory argument suggests that a POSITA *could* configure Gennaro's system to perform its authentication scheme in response to receiving a request to use a file in a predefined way, not that a POSITA *would have been motivated* to do so. *Belden Inc. v. Berk–*

Tek LLC, 805 F.3d 1064, 1073 (Fed. Cir. 2015) ("[O]bviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention.") Accordingly, Petitioner does not provide a sufficient motivation to modify Gennaro as proposed.

For the above reasons, Petitioner fails to show that Gennaro discloses the Limitation 42[a] "receiving a request to use the file in a predefined way."

C. Gennaro Fails to Disclose Limitation 42[e]

Gennaro also fails to disclose Limitation 42[e]: "granting the request to use the file in the predefined way." As an initial matter, this claimed step must be performed in Gennaro: that is, the same entity *receiving* the request to use the file in a predefined way must also "*grant*" that request. This does not happen in Gennaro. Performing the "granting" step is not the same thing as taking no action to stop an ongoing process. Petitioner's fatally flawed contentions repeatedly equate the two. In addition, not only does Petitioner fail to identify an express disclosure of the "granting" step in Gennaro, it also fails to provide any evidence of a "suggestion or motivation to modify the teachings of that reference" to add such a step, as required to support its obviousness challenge. *SIBIA,* 225 F.3d at 1356. Ground 2 should be rejected for this reason alone.

Petitioner first argues that Gennaro at 2:54, 2:65-67 "disclose[s] that the receiver plays a stream, thus granting the user's request to play an internet application." Petition at 56. Not so. The cited portions of Gennaro merely explain that finite streams of data, such as "digital movies, digital sounds, [and] applets," can be processed according to Gennaro's system. *See* Ex. 1008 at 2:64-3:4; Ex. 2027 at ¶192. But even if the cited portions described the playback of a data stream, there is no disclosure that the system takes an affirmative step to *grant* any request to use a file in a predefined way. Ex. 2027 at ¶193. This is evidenced by Gennaro itself, which merely allows the processing of authenticated blocks of the data stream to *continue* if no errors are detected in a received block. *See* Ex. 1008 at 5:54-63 (if an error is detected the processing of the block is "halted," "[o]therwise" the processing of the block continues); Ex. 2027 at ¶193. Gennaro describes an iterative process that divides the stream into blocks, and authenticates each block individually. Ex. 2027 at ¶194. Hence, like Hanna discussed above, Gennaro describes that some portions of the stream may be verified, while other are not. *Id*. If verified, the MPEG software is informed of the block and "it can proceed to process the incoming original block that was authenticated."[14] *Id*. Conversely, the MPEG software is not

[14] This processing of authenticated blocks by the MPEG software (not further described in Gennaro) may include performing methods, such as those disclosed in the '815 patent, that process requests by the recipient to use the block in a predefined

informed of any blocks that cannot be authenticated, and those corrupted portions of the stream are not further processed. Ex. 2027 at ¶195. In such a system as Gennaro that verifies the stream in a block-by-block manner, it is unclear what it would even mean "to *grant* a request to use a file in a predefined way," as all of the file may not be further processed by the MPEG software for use. *Id*. Moreover, that Gennaro's processing of a block can be halted at any time tampering is detected shows that there is no single step performed that "grants" the use of the file in a predefined manner.[15] *Id*.

Finally, Petitioner contends that Limitation 42[e] is disclosed because a prior art receiver "asks for the authenticated stream." Petition at 56 (citing Ex. 1008 at 1:28-29). But even if a POSITA would rely on this portion of Gennaro that criticizes the prior art to modify Gennaro's own system, simply requesting an authenticated stream is not the same thing as *granting* a request to "*use* the file *in a predefined manner*." There is no disclosure in Gennaro of its system "granting" a request to provide an authenticated stream, nor is providing an authenticated stream a "use" of

---

manner, but there is no such suggestion or motivation in Gennaro regarding managing the use of the block, nor is a block a "file."

[15] Dr. Madisetti testified that "the web server that's originating the internet movie" could grant the request to play the video "when it allows the stream to be sent"; in other words, before any block of the stream is even authenticated. Ex. 2026 at 267:24-268:7. This would defeat the purpose of Gennaro's stream signing method.

that stream. Ex. 2027 at ¶196. As explained above, authentication by Gennaro's system is a prerequisite for processing the blocks of the stream for use. Ex. 1008 at 5:8-12 (the blocks must be authenticated "before passing them on to the MPEG processing software **(2.200)** to be converted back to video using the MPEG standard.") Ex. 2027 at ¶196.

Accordingly, Petitioner fails to show that Gennaro discloses Limitations 42[a] and 42[e]. Ground 2 should be denied.

IX. DEPENDENT CLAIM 43

Claim 43 depends from independent claim 42 and, therefore, includes all of the features and limitations of claim 42. Accordingly, Petitioner fails to show that claim 43 is unpatentable in Grounds 1 and 2 for at least the same reasons provided above with respect to claim 42, and for its own unique features and limitations. Ex. 2027 at ¶198.

X. CONCLUSION

In view of the foregoing, Patent Owner respectfully requests that the Petition for *Inter Partes* Review of the '815 patent be denied.

Date: January 21, 2021

Respectfully submitted,

By: /s/ *Christopher A. Mathews*
Christopher A. Mathews (Reg. No. 35,944)
QUINN EMANUEL URQUHART & SULLIVAN, LLP
865 S. Figueroa St.
Suite 1000
Los Angeles, CA 90017
213.443.3000
213.443.3100
Email: chrismathews@quinnemanuel.com

Lead Attorney for Patent Owner – Intertrust Technologies Corp.

CERTIFICATE OF COMPLIANCE

I hereby certify that this paper complies with the type-volume limitation of 37 C.F.R. § 42.24 because it contains 12,817 words, excluding the parts of the paper exempted by 37 C.F.R. § 42.24(b).

/s/ Christopher A. Mathews

Christopher A. Mathews
Registration No. 35,944

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), the undersigned hereby certify that PATENT OWNER'S RESPONSE, and all exhibits and other documents filed together with the response, were served on January 21, 2021 by e-mailing copies to:

Lead Counsel	Back-Up Counsel
Scott A. McKeown Reg. No. 42,866 ROPES & GRAY LLP 2099 Pennsylvania Avenue, NW Washington, D.C. 20006-6807 Phone: 202-508-4740 Fax: 617-235-9492 scott.mckeown@ropesgray.com **Mailing address for all PTAB correspondence:** ROPES & GRAY LLP IPRM—Floor 43 Prudential Tower 800 Boylston Street Boston, Massachusetts 02199-3600	Mark Rowland Reg. No. 32,077 Keyna Chow *Pro Hac Vice Forthcoming* ROPES & GRAY LLP 1900 University Ave., 6th Floor East Palo Alto, CA 94303-2284 Phone: 650-617-4000 Fax: 617-235-9492 mark.rowland@ropesgray.com keyna.chow@ropesgray.com Leslie Spencer Reg. No. 47,105 Desmarais LLP 230 Park Ave. New York, NY 10169 Phone: 212-351-3400 Fax: 212-351-3401 lspencer@desmaraisllp.com

Date: January 21, 2021

Respectfully submitted,

By: /s/ *Razmig Messerian*

Razmig Messerian (Reg. No. 56,983)
QUINN EMANUEL URQUHART & SULLIVAN, LLP
865 S. Figueroa St.
Suite 1000
Los Angeles, CA 90017
213.443.3000
213.443.3100
Email: razmesserian@quinnemanuel.com

Attorney for Patent Owner – Intertrust Technologies Corp.