Trials@uspto.gov
571-272-7822

Paper 49
Entered: December 18, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SEAGATE TECHNOLOGY (US) HOLDINGS, INC., and
SEAGATE TECHNOLOGY LLC,
Petitioner,

v.

ENOVA TECHNOLOGY CORP.,
Patent Owner.

Case IPR2014-01178
Patent 7,900,057 B2

Before MICHAEL R. ZECHER, GEORGIANNA W. BRADEN, and TIMOTHY J. GOODSON, *Administrative Patent Judges.*

GOODSON, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Seagate Technology (US) Holdings, Inc. and Seagate Technology LLC (collectively, "Petitioner") filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 1–32 of U.S. Patent No. 7,900,057 B2 ("the '057 patent," Ex. 1001). Enova Technology Corporation ("Patent Owner") timely filed a Preliminary Response to the Petition. Paper 9. Based on these submissions, we instituted trial as to claims 1–32 of the '057 patent on the following proposed ground of unpatentability: Claims 1–32 as unpatentable under 35 U.S.C. § 103(a) over Sullivan[1] and SATA Standard.[2] Paper 10, 18 ("Dec. to Inst.").

After institution, Patent Owner filed a Patent Owner's Response (Paper 26, "PO Resp."), and Petitioner filed a Reply (Paper 28, "Reply"). Patent Owner also filed a Motion to Seal Exhibits 2042, 2043, and 2044, which is addressed herein. Paper 25 ("Mot. to Seal").

An oral hearing was conducted on November 2, 2015. A transcript of the oral hearing is included in the record. Paper 48 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(c). This decision is a Final Written Decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 as to the patentability of claims 1–32. For the reasons discussed below, Petitioner has demonstrated by a preponderance of the evidence that these claims are unpatentable.

A. Related Proceedings

Petitioner indicates the '057 patent currently is the subject of a related

[1] U.S. Patent Publication No. 2004/0054914 A1, published Mar. 18, 2004 (Ex. 1002, "Sullivan").

[2] *Serial ATA: High Speed Serialized AT Attachment*, Serial ATA Workgroup, Rev. 1.0a, Jan. 7, 2003 (Ex. 1003, "SATA Standard").

proceeding between the parties in the U.S. District Court for the District of Delaware titled *Enova Tech. Corp. v. Seagate Tech. (US) Holdings, Inc.*, No. 1:13-cv-1011-LPS. Pet. 1. Petitioner also represents the ’057 patent was the subject of a prior proceeding in the U.S. District Court for the District of Delaware titled *Enova v. WD*, No. 1:10-cv-00004-LPS. *Id.*

The ’057 patent is the subject of *inter partes* reviews involving the same parties in Cases IPR2014-01297 and IPR2014-01449. Additionally, Case IPR2014-00683 involved the same parties and related U.S. Patent No. 7,136,995 B1 (“the ’995 patent”). Another panel of this Board mailed a Final Written Decision in Case IPR2014-00683, in which they determined that the Petitioner in that proceeding demonstrated by a preponderance of the evidence that claims 1–15 of the ’995 patent are unpatentable. *Seagate Tech. (US) Holding, Inc. v. Enova Tech. Corp.*, Case IPR2014-00683 (PTAB Sept. 2, 2015) (Paper 47).

B. The ’057 Patent

The ’057 patent relates to a cryptographic serial Advanced Technology Attachment (ATA) apparatus and method. Ex. 1001, Title, 1:33–40. The ’057 patent also refers to serial ATA as “SATA.” *Id.* at 1:44–45. The ’057 patent discloses that the SATA specification defines a point-to-point connection between a host adapter, such as an integrated circuit, and a storage device controller, such as a SATA hard-disk drive. *Id.* at 1:49–56. According to the ’057 patent, the SATA specification also provides for layering of functions and includes a Link layer “responsible for delivering packets of payload data, which are called Frame Information Structures (FISes).” *Id.* at 2:46–48.

Figure 1 is reproduced below.

FIG. 1

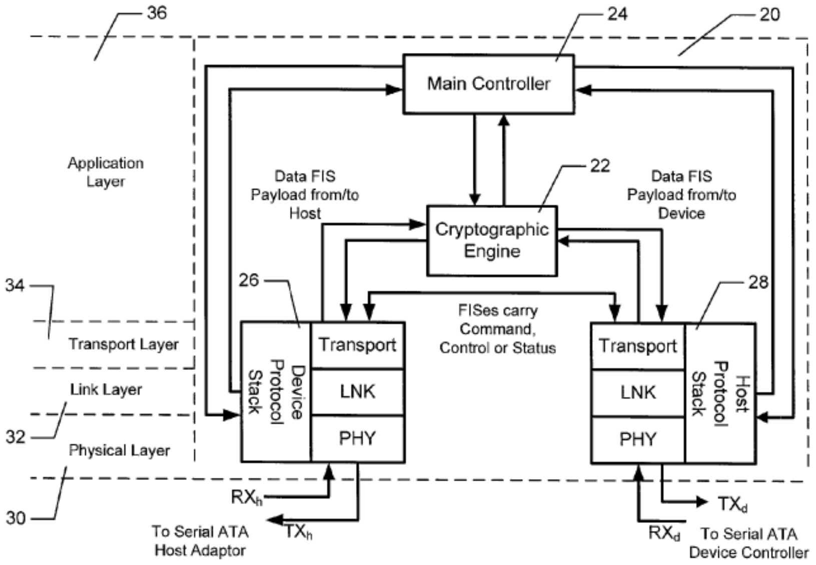

Figure 1 depicts a block diagram of cryptographic SATA apparatus 20 configured to receive input RX_h from and transmit output TX_h to a SATA host adapter. *Id.* at 5:40–42. The SATA host adapter or host may be provided on a host personal computer (PC). *Id.* at 5:42–44. Figure 1 also shows that cryptographic SATA apparatus 20 is configured to receive input RX_d from and transmit output TX_d to a SATA device controller. *Id.* at 5:44–47. The SATA device controller or device may be provided on a peripheral device, such as a hard disk drive, optical drive, or the like. *Id.* at 5:47–51. The ’057 patent indicates that cryptographic SATA apparatus 20 communicates with the host and the device through appropriate communicative coupling (e.g., SATA cables). *Id.* at 5:51–53.

As further shown in Figure 1, cryptographic SATA apparatus 20 includes cryptographic engine 22 operatively coupled between main controller 24 and device and host protocol stacks 26 and 28. Ex. 1001, Fig. 1. Main controller 24 regulates all signal paths that carry data, command, control, and status signals. *Id.* at 6:12–13. Main controller 24 further regulates the operation of cryptographic engine 22. *Id.* at 6:21–23.

Cryptographic engine 22 performs encryption/decryption operations on predefined and/or selected data FIS payloads exchanged between the host and the device. Ex. 1001, 6:1–3. Non-data FISes or data FISes that do not require encryption/decryption, such as FISes carrying command, control or status information, are allowed to pass straight through SATA apparatus 20, thereby bypassing cryptographic engine 22. *Id.* at 6:3–8, 7:30–33. SATA apparatus 20 may be configured to examine the FIS type field (i.e., the first byte of the received FIS header) to determine FIS type. *Id.* at 6:40–43. An FIS type detector may be provided in Transport layer 34 or in Link layer 32 to determine FIS type. *Id.* at 6:43–45, 7:67–8:8.

C. Illustrative Claim

Of the challenged claims, claim 1 is independent. Claims 2–32 depend, directly or indirectly, from claim 1. Claim 1 is illustrative of the challenged claims, and is reproduced below:

> 1. A cryptographic Serial ATA (SATA) apparatus, comprising:
>
> a SATA protocol stack for communicating with an interface of a device;
>
> a cryptographic engine operatively coupled to the SATA protocol stack for encrypting or decrypting at least a subset of data FISes (Frame Information Structures) communicated to or from the SATA protocol stack; and
>
> a main controller implemented at least partially in hardware, the main controller configured to cause:
>
> > the SATA protocol stack to send at least first payload of a first data FIS to the cryptographic engine responsive to the first data FIS associated with a predefined category of command set;

> the cryptographic engine to decrypt at least a portion of the first payload received from the SATA protocol stack; and
>
> the SATA protocol stack to process a Register-Device to Host FIS without decryption responsive to receiving the Register-Device to Host FIS from the interface of the device.

Ex. 1001, 13:6–26.

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see also In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1275–79 (Fed. Cir. 2015) (holding that "Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA" and "the standard was properly adopted by PTO regulation"). Under that standard, and absent any special definitions, we give claim terms their ordinary and customary meaning, as would be understood by one of ordinary skill in the art, in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

In the Decision to Institute, we construed "SATA protocol stack" in claims 1 and 8 to mean "a set of SATA protocols that work together on different levels to enable communication on a network." *See* Dec. to Inst. 6–8. In its Response, Patent Owner argues for the construction of this term that the District Court adopted in *Enova v. WD*, which was "one or more of a physical, a link and a transport layer and does not include the application layer." PO Resp. 15 (citing Ex. 2064; Ex. 2061 ¶¶ 68–69). Patent Owner asserts that the District Court's construction "better captures the meaning according to one of skill in the art, because it captures the layers described in the SATA Standard itself." *Id.*

Patent Owner does not point to any support in the Specification for its proposed construction, nor does Patent Owner persuasively address the reasoning provided in the Decision to Institute for the construction we initially adopted for purposes of this proceeding. *See id.* The District Court's claim construction order on which Patent Owner relies includes little persuasive support for Patent Owner's position here. *See* Ex. 2064 ¶ 6. Moreover, Patent Owner does not contend that the difference between its proposed construction and the construction in the Decision to Institute has any impact on the obviousness analysis in this proceeding. *See* PO Resp. 15–16 (asserting that the Petition fails to demonstrate obviousness under either the construction adopted in the Decision to Institute or Patent Owner's proposed construction); Tr. 88:4–23.

Accordingly, Patent Owner does not provide a persuasive reason to alter the construction of "SATA protocol stack" that we set forth in the Decision to Institute. Therefore, for the reasons set forth in the Decision to Institute, we maintain our construction of "SATA protocol stack" in claims 1 and 8 as "a set of SATA protocols that work together on different levels to enable communication on a network."

B. Principles of Law

To prevail in its challenges to the patentability of the claims, a petitioner must establish facts supporting its challenges by a preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved based on underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere*, 383 U.S. 1, 17–18 (1966). We also recognize that prior art references must be "considered together with the knowledge of one of ordinary skill in the pertinent art." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citing *In re Samour*, 571 F.2d 559, 562 (CCPA 1978)).

We analyze the instituted ground of unpatentability in accordance with the above-stated principles.

C. Level of Skill in the Art

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, and the sophistication of the technology. *Custom Accessories, Inc. v. Jeffrey-Allan Indus. Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986). Also, we are guided by the level of skill in the art as reflected by the prior art of record. *Okajima v. Bourdeau*, 261 F.3d. 1350, 1355 (Fed. Cir. 2001).

Petitioner contends that a person of ordinary skill in the field of this invention would have had at least a bachelor's degree in electrical engineering, computer engineering, or computer science, and two years of experience in a relevant field, or equivalent knowledge and experience. Pet.

3–4 (citing Ex. 1006 ¶¶ 16–17). Patent Owner’s Response does not address specifically the level of ordinary skill in the art. We note, however, that Patent Owner’s declarant, Dr. Thomas A. Conte, testifies that, because the claims of the ’057 patent describe a cryptographic apparatus, which is a computer hardware device, one of ordinary skill in the art should have experience with the hardware of devices and systems. Ex. 2061 ¶ 18.

Dr. Conte’s testimony does not persuade us that hardware encryption experience is a prerequisite for the level of ordinary skill, such that persons having a software background or a degree in computer science are excluded from being persons of ordinary skill. *See id.* Although the Specification of the ’057 patent and the challenged claims disclose a “cryptographic device,” the ’057 patent teaches that “[t]he above-described embodiments may be implemented in hardware and/or software form, as desired.” Ex. 1001, 12:10–11.

After considering the evidence of record, we conclude that a person of ordinary skill in the art at the time of the ’057 patent would have had a bachelor’s degree in electrical engineering, computer engineering, or computer science, and at least two years of experience.

D. Claims 1–32 – Obviousness over Sullivan (Ex. 1002) and SATA Standard (Ex. 1003)

Petitioner argues claims 1–32 are unpatentable under 35 U.S.C. § 103(a) over Sullivan and SATA Standard. Pet. 23–59. Patent Owner contests Petitioner’s position. PO Resp. 16–60. As explained below, we have considered the arguments and evidence presented by both parties, and we determine that Petitioner has shown by a preponderance of the evidence that claims 1–32 are unpatentable over Sullivan and SATA Standard.

1. Summary of Sullivan (Ex. 1002)

Sullivan relates to a method and apparatus for in-line serial data encryption. Ex. 1002, Title. Sullivan describes the encryption of data transmitted from a host computer to a target device, such as a storage system, where the encryption is carried out in-line with the data channel. Ex. 1002 ¶ 2.

Figures 1 and 9 are reproduced below.

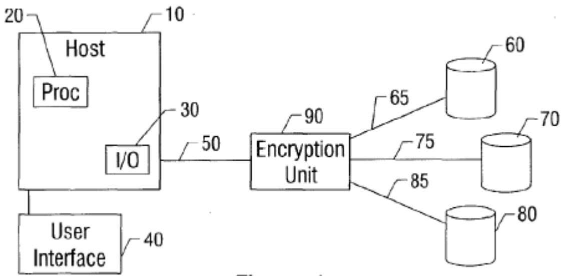

Figure 1

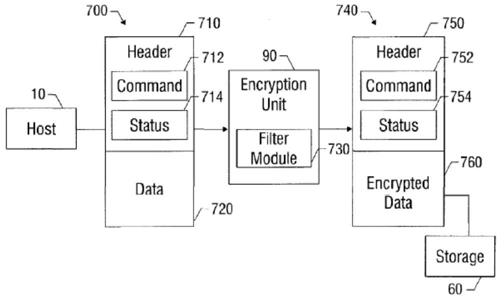

Figure 9

Figure 1 depicts processor-based system 10, which includes subsystem 30 in communication with serial channel or bus 50. Ex. 1002 ¶ 21. Sullivan discloses "[t]he serial channels . . . may be any of a number of other suitable serial channels, such as serial ATA." *Id.* ¶ 38. Storage devices 60–80 are connected to serial channel 50 via encryption unit 90. *Id.* ¶ 22. Figure 9 depicts encryption unit 90 with filter module 730 configured to pass only a predetermined set of commands, status, or other information included in header 710. *Id.* ¶ 55. "Alternatively or additionally, the filter module may include logic configured to reject a predetermined set of information or categories of information, e.g. to reject certain types of data, address pointers, and so on." *Id.* Figure 9 depicts packet 700 transmitted to encryption unit 90 from host 10. *Id.* at Fig. 9. Packet 700 includes header 710 with command information 712, status information 714, and data

720. *Id.* ¶ 54.

Additionally, as shown in Figure 2, Sullivan further discloses encryption unit 90 may include processor 100, memory 105, encrypt module 110, and transmit module 120. Ex. 1002 ¶ 23. Sullivan teaches an encrypt module may be configured to "encrypt the data bits and to leave the control information substantially unaltered." *Id.* at claim 1.

2. Summary of SATA Standard (Ex. 1003)

SATA Standard, titled "Serial ATA: High Speed Serialized AT Attachment," is directed to providing a "technical specification of a high-speed serialized ATA data link interface." Ex. 1003, 11. SATA Standard discloses that "[s]erial ATA is a high-speed serial link replacement for the parallel ATA attachment of mass storage devices." *Id.* at 23.

SATA Standard discloses that information may be transferred between a host and a device through FISes. Ex. 1003, 184, 199. SATA Standard includes several different types of FISes, which are used for different purposes. *See id.* at 185–200. The FIS type is indicated by the value in a designated field of the FIS.

For example, SATA Standard specifies that a "Register-Device to Host FIS" is indicated when the FIS Type field is set to a value of 34h. Ex. 1003, 188. This FIS Type is used "by the device to update the contents of the host adapter's Shadow Register Block. This is the mechanism by which devices indicate command completion status . . . ." *Id.*

As another example, a value of 46h in the FIS Type field indicates a Data FIS, which is "used for transporting payload data, such as the data read from or written to a number of sectors on a hard drive." Ex. 1003, 199. SATA Standard describes that "[t]his FIS is generally only one element of a sequence of transactions leading up to a data transmission and the transactions leading up to and following the Data FIS establish the proper context for both the host and device." *Id.*

In addition, SATA Standard describes several command classes, which are groups of specified commands that share a common sequence of transfers in the execution of the command. *See, e.g.*, Ex. 1003, 248–54. Two such command classes are Programmed Input/Output (PIO) data-out and Direct Memory Access (DMA) data-in. *Id.* at 252–53.

3. Claims 1–4, 6, 8, 10–15, and 20–27

The Petition argues that each limitation of claim 1 is rendered obvious by Sullivan in combination with SATA Standard. *See* Pet. 24–35. In rebutting Petitioner's arguments and evidence regarding claim 1, Patent Owner's Response focuses on the limitation that the main controller is configured to cause the SATA protocol stack to send at least a first payload of a first data FIS to the cryptographic engine "responsive to the first data FIS associated with a predefined category of command set." Ex. 1001, 13:17–19; *see* PO Resp. 16–45. For convenience, we refer to this limitation as the "associated with" limitation.

Petitioner argues that the "associated with" limitation would have been obvious to a skilled artisan implementing Sullivan's teachings using SATA Standard. *See* Pet. 28–33. Specifically, Petitioner asserts that Sullivan teaches that the encryption unit encrypts data to be stored on the storage device. *Id.* at 29 (citing Ex. 1002 ¶¶ 35, 47, 70). Sullivan also teaches that control information, including command and status information, is not encrypted. *Id.* at 30 (citing Ex. 1002, Abstract; ¶ 6, claim 1, claim 9). Based on these disclosures, Petitioner's declarant, Dr. Long, testifies that:

> Sullivan thus reflects the concept well known to persons of ordinary skill in the art at the time the ’057 Patent was filed . . . that user data is stored on a storage device and is suitable for encryption, but control information is used by the device, must be readable by the device, and should not be changed because encrypting that information would render the information unusable or unreadable.

Ex. 1006 ¶ 104.

Turning to SATA Standard, Dr. Long testifies that SATA Standard “specifies the sequence of FISes transmitted between the host and the device in order to execute a particular command.” *Id.* at ¶ 96. In particular, Dr. Long explains that:

> [I]n SATA, execution of a particular command triggers the transmission of Data FISes and dictates the contents of those Data FISes. . . . For example, the “READ SECTOR(S)” command will be associated with a Data FIS containing user data previously stored on and read from the disk. In contrast, the “IDENTIFY_DEVICE” command will be associated with a Data FIS containing control information. Although the execution of both of these commands involves the transfer of Data FISes . . . , the commands associated with each Data FIS require different types of information (*i.e.*, control information or user data) to be included in the Data FIS.

Id. at ¶ 101. Dr. Long’s declaration includes an exemplary list of commands in SATA Standard that are for reading user data from the hard drive or writing user data to the hard drive. *Id.* at ¶ 99 (citing Ex. 1003, 250–55).

Thus, Petitioner argues that it would have been obvious to configure Sullivan’s main controller to send the payload of a Data FIS to the cryptographic engine when that Data FIS is associated with a read or write command from a pre-defined group of read or write commands in SATA. Pet. 31 (citing Ex. 1006 ¶¶ 154–55). The motivation for doing so, according to Petitioner, would have been to achieve the predictable result of encrypting or decrypting user data while leaving control information unaltered. *Id.*

Petitioner also points to Sullivan's description of a filter module in the interface of the cryptographic core to act as a "command pass filter" for passing "only a predetermined allowed set of commands." Pet. 32 (citing Ex. 1002 ¶¶ 55, 64–65). Petitioner notes Sullivan's description that "[t]ypical allowed commands will be read, write, and other commands associated with data or memory access and storage." *Id.* (quoting Ex. 1002 ¶ 56). Petitioner argues that Sullivan's filter, when implemented in SATA, would allow only Data FISes sent pursuant to those approved commands to reach the cryptographic core for encryption or decryption. *Id.* at 32–33 (citing Ex. 1006 ¶ 156). Thus, according to Petitioner, a skilled artisan would have appreciated that Sullivan's filter could be used to encrypt or decrypt only data associated with a predetermined allowed set of commands, such as read and write commands, in order to encrypt or decrypt data to be written to or read from a storage device without encrypting command, control, or status information. *Id.* at 33 (citing Ex. 1006 ¶ 156).

Patent Owner argues that the "associated with" limitation would not have been obvious based on the cited combination for at least two reasons. First, Patent Owner argues that Sullivan does not teach associating a pre-defined category of command set. PO Resp. 19–34. In presenting this argument, Patent Owner asserts that "the encryption approach described in Sullivan is a simple solution tied to the kinds of packets described by Sullivan." *Id.* at 22. Specifically, "Sullivan teaches that the 'control information' in the disclosed serial 'packets' is in the header. 'The data is separated from the header, encrypted, recombined with the header, and transmitted to the target device.'" *Id.* at 24 (quoting Ex. 1002 ¶ 9). Patent Owner points out that, like the packets described in Sullivan, FISes have headers and bodies as well. *Id.* (citing Ex. 1006 ¶ 70). Thus, Patent Owner argues that "[t]he disclosure of Sullivan, as applied to the SATA Standard, is a discussion of the internals of **every** FIS; it does not teach to differentiate between payloads in any way." *Id.* (citing Ex. 2061 ¶ 96). According to Patent Owner, following this approach of treating every FIS in the same way by encrypting the header of each FIS would result in a non-functional system. *Id.* at 25–26.

Patent Owner further argues that Sullivan's description of the command pass filter does not teach the "associated with" limitation because Sullivan's filter "does not associate Data FISes with the category of command set at all." PO Resp. 29. Rather, according to Patent Owner,

> the filter module of Sullivan examines information in a given packet and then determines whether it will allow **that packet** to pass through to the encryption engine or not, at which point, if allowed to pass, the data in the payload of the packet **in which the very same control information appears** is encrypted. If not allowed to pass, the entire packet is rejected and dropped.

Id. (emphasis added) (citing Ex. 2061 ¶ 103). Patent Owner argues, with citation to Dr. Conte's declaration, that if Sullivan's filter were implemented in certain sequences of FISes in a SATA device, the result would be to encrypt the payloads of FISes that should not be encrypted and to reject other FISes that should be encrypted. *Id.* at 30–32 (citing Ex. 2061 ¶¶ 46, 105, 106).

Patent Owner's next argument for why the cited combination does not render obvious the "associated with" limitation is that SATA Standard does not teach the limitation. *See* PO Resp. 34–45. Patent Owner asserts that

"SATA Standard is silent as to the use of encryption and teaches nothing about whether a data payload should be decrypted or encrypted." *Id.* at 34 (citing Ex. 2061 ¶ 107). Patent Owner challenges Petitioner's contention that a skilled artisan "would have appreciated that Sullivan, when implemented in SATA, teaches decrypting the payload of a Data FIS when that Data FIS is associated with one of SATA's read commands." *Id.* at 35 (quoting Pet. 29). Patent Owner argues that the association of a Data FIS with a read or write command could not be used to determine whether to encrypt or decrypt the Data FIS's payload because "there are several read and write commands in the SATA Standard that would result in Data FISes whose payloads should not be cryptographically processed." *Id.* For example, Patent Owner asserts that Data FISes transmitted in response to SMART READ LOG SECTOR should not be cryptographically processed because they contain data relating to the drive's operation. *Id.* at 35–36 (citing Ex. 2061 ¶ 108; Ex. 1003, 250, 252).

Patent Owner also takes issue with Dr. Long's list of commands in SATA Standard for reading user data from the hard drive and for writing user data to the hard drive. *See* PO Resp. 36; Ex. 1006 ¶ 99. Patent Owner states that Dr. Long's deposition testimony establishes that Dr. Long did not assemble this list himself and that the list does not exist in the same form in SATA Standard itself. *Id.* at 36–37 (citing Ex. 2060, 41:5–14, 42:11–22). Patent Owner contends that "neither Sullivan nor the SATA Standard alone provide enough information to determine which commands carry command, control, or status information and which ones do not, since the purpose of the commands is not found in the SATA Standard." *Id.* at 37 (citing Ex. 2061 ¶ 34). Furthermore, Patent Owner notes that "the ATA Standard, a predecessor of the SATA Standard, is not one of the two references" in the ground on which this proceeding was instituted. *Id.*

We do not find Patent Owner's arguments summarized above to be persuasive. As an initial point, we agree with Petitioner that Patent Owner's primary arguments attack the two references individually instead of considering what these references together would teach to a skilled artisan. *See* Reply 2–3 (citing *In re Merck*, 800 F.2d 1091, 1097 (Fed. Cir. 1986)). Here, Petitioner is not relying on either Sullivan or SATA Standard individually as teaching the "associated with" limitation. Rather, Petitioner's obviousness case against claim 1, as summarized above, is premised on the notion that the "associated with" limitation would have been obvious to a skilled artisan seeking to implement Sullivan's teachings—specifically, Sullivan's teaching to encrypt or decrypt user data but not control information—in a SATA device. Patent Owner's arguments that neither Sullivan nor SATA Standard individually teaches the "associated with" limitation do not address directly the obviousness case that Petitioner has presented.

Furthermore, Patent Owner's arguments take an unduly narrow view of Sullivan's teachings. Specifically, Patent Owner's arguments are premised on the view that a skilled artisan would have understood from Sullivan's teachings that each packet must be treated identically for encryption purposes. We are not persuaded that a skilled artisan would have understood Sullivan in that way, especially when Sullivan's teachings are implemented in a SATA device as in the proposed combination. On this point, we note that Patent Owner does not cite (and we do not find) any disclosure in Sullivan expressly stating that every packet should be treated the same way in carrying out the encryption operation. *See* Tr. 74:13–75:13. Instead, Patent Owner infers from Sullivan's disclosure that all individual packets must be treated the same way because Sullivan teaches only one way to process packets for encryption—i.e., by removing control information in the header of a packet and encrypting the payload. *See id.*; PO Resp. 19 (citing Ex. 1002 ¶¶ 39, 47), 24 (citing Ex. 1002 ¶ 9).

However, Patent Owner's reading of Sullivan does not account adequately for the disclosure in Sullivan that is broader and more general. For example, in the Background section, Sullivan describes that "[a] system is needed whereby transmission of data in a serial channel can be accomplished in-line and in real time, ***where the data and control information can be treated separately for*** both ***encryption purposes*** and for handling various types of attacks and covert processes embedded in or achieved by the transmitted information." Ex. 1002 ¶ 6 (emphasis added); *see also id.* at ¶ 10 ("The control information, which may include commands and status information, can be subjected to filtering and rejecting operations by the encryption unit, to pass through only a predetermined set of commands and/or to reject a predetermined set of commands."); *id.* at ¶ 55 ("[T]he filter module 730 may be configured as an information or command pass filter or blocking filter for ***any control information that may be included in the packet 700, whether or not in the header***.") (emphasis added); *id.* at claim 9 ("transmitting the encrypted information with the associated control information to the second device, where the associated control information is transmitted in an unencrypted form"). In view of these teachings, we agree with Petitioner that "Sullivan describes making encryption decisions based on the ***type*** of data and not simply the ***location*** of the data (e.g., in a header or in a payload)." Reply 8.

Further, a skilled artisan would not have understood Sullivan's teaching to strip out the header and encrypt the payload as a prescription for how each individual FIS should be treated when Sullivan is applied to a SATA device, because that encryption strategy would yield a non-functioning SATA device. It is undisputed that implementing Sullivan in a SATA device in this manner would result in a non-functional system, because doing so would result in encryption of payloads that should not be encrypted, thereby rendering the FISes unintelligible to the host or the peripheral device intended to process them. *See* PO Resp. 26; Reply 9. As summarized above, Patent Owner argues that this non-functionality demonstrates a flaw in Petitioner's proposed combination. *See* PO Resp. 26. Yet, we view Patent Owner's argument regarding non-functionality as detracting from the persuasiveness of Patent Owner's contentions regarding how a skilled artisan would have understood Sullivan's disclosure. In particular, it strains credulity that a skilled artisan would apply Sullivan in the manner Patent Owner urges when doing so would result in a non-functioning device.

We agree with Petitioner that an artisan having ordinary skill and creativity would not have applied Sullivan's teachings in such a simplistic and plainly counterproductive fashion. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007) ("A person of ordinary skill is also a person of ordinary creativity, not an automaton."); *see also* Reply 9 (citing *In re Sovish*, 769 F.2d 738, 743 (Fed. Cir. 1985); *Scanner Techs. Corp. v. ICOS Vision Sys. Corp.*, 528 F.3d 1365, 1382 (Fed. Cir. 2008)). We further agree with Petitioner that a skilled artisan would recognize that "Sullivan teaches a flexible cryptographic device that can be implemented using a variety of data transfer protocols . . . and is designed to 'accommodate[] whatever standard is used.'" Reply 8 (quoting Ex. 1002 ¶ 50).

Thus, although Sullivan describes encryption operations for a single packet, a skilled artisan would have appreciated that SATA devices utilize prescribed sequences of FISes to transfer data. *See* Ex. 1006 ¶¶ 95–103 (summarizing data transfer operations in SATA Standard and noting that "SATA Standard . . . specifies the sequence of FISes transmitted between the host and the device in order to execute a particular command."); Ex. 2061 ¶ 42 ("The command protocols dictate a prescribed sequence of FIS transmissions, which Dr. Long describes in his declaration. I generally agree with Dr. Long's recitation of the order of FISes for various operations."). As Dr. Long explained succinctly in his deposition testimony:

> Sullivan is a fairly high-level disclosure in that it talks about packets in the generic sense. And when implemented in SATA, that gets turned into a transaction, which is a sequence of FISes going back and forth. . . . Sullivan says this can be implemented in SATA. In order to implement this in SATA, the SATA protocol defines that what would be a packet in Sullivan becomes a transaction.

Ex. 2060, 79:13–80:1.

With respect to how Sullivan's teachings would be implemented in a SATA device, we find persuasive Petitioner's explanation that a skilled artisan would have found it obvious to distinguish between Data FISes that carry user data and Data FISes that carry control, command, or status information, by utilizing the association in SATA Standard between a given command and the type of information in a resulting Data FIS. *See* Pet. 29, 31; Ex. 1006 ¶¶ 30–35, 50, 101–03, 154; Reply 5–6.

Patent Owner's second argument is unpersuasive because it is based on a misunderstanding of Petitioner's obviousness case. To recapitulate Patent Owner's second argument, Patent Owner identifies certain commands in SATA Standard, such as SMART READ LOG SECTOR, that result in Data FISes whose payloads should not be encrypted. PO Resp. 35–36. According to Patent Owner, this point rebuts Petitioner's contention that the association of a Data FIS with a read or write command could be used to determine whether to encrypt or decrypt the Data FIS's payload. *Id.* (citing Pet. 29). However, as discussed above, Petitioner's proposed combination relies on the association in SATA Standard between commands that call for the transfer of user data and the resulting Data FIS with user data in its payload. *See* Pet. 31; Ex. 1006 ¶¶ 50, 101, 154; Reply Br. 5–6. Petitioner further provides an articulated reason with a rationale underpinning explaining why it would be obvious to utilize this association–namely, to separate user data from control information for encryption purposes, as taught by Sullivan. *See* Pet. 31; Ex. 1002 ¶ 6. We agree with Petitioner that "Patent Owner provides no rationale for why a skilled artisan would have been misled into thinking a command transfers user data simply because the name of the command includes the word 'read' or 'write.'" Reply 13 (citing Ex. 2060, 22:12–20, 43:3–13; Ex. 2061 ¶ 41).

In this regard, we are not persuaded by Patent Owner's contention that SATA Standard does not provide enough information for a skilled artisan to determine which commands call for the transmission of control information and which commands call for user data. *See* PO Resp. 37. Rather, we agree with Petitioner that identifying the commands in the SATA Standard that transfer user data would not have been uniquely challenging or otherwise beyond the level of an ordinary skilled artisan. *See* Ex. 1006 ¶ 155. Dr. Conte testifies that "[t]he purpose and function of the individual commands described by the various command protocols is outside of the scope of the SATA Standard on which the Petition[] rel[ies]; they are described by the ATA specification itself." Ex. 2061 ¶ 41. Yet, SATA Standard lists the ATA specification as a reference "contain[ing] provisions that, through reference in the text, constitute provisions of this standard." Ex. 1003, 13. Dr. Conte also testifies that "[t]he SATA protocol was developed as a high-speed replacement for the then-popular ATA protocol." Ex. 2061 ¶ 27; *see also id.* at ¶ 54 (explaining the use of "legacy ATA commands" in a SATA device); PO Resp. 5 ("SATA emulates the same ATA commands."). Given the popularity of the ATA protocol, commonly used ATA commands would have been familiar to the skilled artisan by the time SATA Standard was adopted. *See* Ex. 2061 ¶ 27.

We note Dr. Conte's testimony that a skilled artisan would not have been generally familiar with the purpose of ATA commands because "[i]t's a large standard. One of ordinary skill in the art would have to study the ATA standard." Ex. 1041, 27:22–25. Yet in this respect, Dr. Conte's testimony is consistent with Dr. Long's testimony that in order to determine which SATA commands transfer user data and which transfer non-user data, "[s]ome of them are just really obvious, and other ones we would look at the ATA spec because nobody memorizes all the commands." Ex. 2060, 91:19–21. The sheer length of SATA Standard and the ATA specification, each of which is over 300 pages, buttresses the testimony of both experts that a skilled artisan would not have committed to memory all of the detail in those standards. *See* Ex. 1003; Ex. 1016.

In our view, this point confirms that persons of ordinary skill in the art would have known to consult the ATA specification to gather information about SATA Standard commands with which they were not already familiar. *See* Ex. 2060, 15:5–9; Tr. 100:7–101:22; *see also Endress + Hauser, Inc. v. Hawk Measurement Sys. Pty. Ltd.*, 122 F.3d 1040, 1042 (Fed. Cir. 1997) ("The person of ordinary skill is a hypothetical person who is presumed to be aware of all the pertinent prior art.") (quoting *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986)). Thus, based on the record before us, we determine that, if a skilled artisan was unfamiliar with a particular command listed in SATA Standard, it would have been routine engineering work to consult the ATA specification to determine whether that command transferred user data or control information.

Patent Owner argues that the ATA specification "is not one of the references in the ground[] allowed by the Board." PO Resp. 37; *see* Ex. 2061 ¶ 41. However, "[a]rt can legitimately serve to document the knowledge that skilled artisans would bring to bear in reading the prior art identified as producing obviousness." *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1365 (Fed. Cir. 2015) (citing *Randall Mfg. v. Rea*, 733 F.3d 1355, 1362–63 (Fed. Cir. 2013)). Petitioner's use of the ATA specification in its obviousness case falls squarely into this category.

We have reviewed Petitioner's contentions and supporting evidence regarding the remaining limitations of claim 1 (Pet. 24–35), which Patent Owner does not address specifically in its Response. Based on the record before us, we conclude that Petitioner has demonstrated by a preponderance of the evidence that independent claim 1 would have been obvious over the combination of Sullivan and SATA Standard.

In addition, upon reviewing the unchallenged contentions and supporting evidence regarding dependent claims 2–4, 6, 8, 10–15, and 20–27 presented in the Petition (Pet. 35–56), we are persuaded that Petitioner presents sufficient evidence to support a finding that the combination of Sullivan and SATA Standard renders obvious the subject matter of these dependent claims. Therefore, we conclude that Petitioner has demonstrated by a preponderance of the evidence that dependent claims 2–4, 6, 8, 10–15, and 20–27 would have been obvious over the combination of Sullivan and SATA Standard.

4. "Bypass" Limitations in Claims 5, 16, 17, and 19

Claims 5, 16, 17, and 19 depend, directly or indirectly, from claim 1. Claim 5 recites that the main controller is configured to send a signal to the cryptographic engine "instructing whether to encrypt, decrypt, or bypass the data FISes received at the cryptographic engine." Ex. 1001, 13:35–40. Claim 16 recites the main controller causes a "decoded FIS to be sent to said cryptographic engine for encryption, decryption, or bypassing." *Id.* at 14:24–26. Claim 17 recites the main controller causes the "decoded FIS to bypass said at least one cryptographic engine." *Id.* at 14: 30–32. Claim 19 recites that the cryptographic engine is "responsive to the bypass flag signal to encrypt, decrypt or bypass a data FIS received by the cryptographic engine." *Id.* at 14:41–44. The parties refer to these limitations as the "bypass" limitations. *See* PO Resp. 45; Reply 19.[3]

[3] Although the use of "or" in the "bypass" limitations of claims 5, 16, and 19 suggests a possibility that it would be sufficient for the controller to instruct

Petitioner argues that for the same reasons as argued with respect to claim 1, a skilled artisan "would have been motivated to encrypt, decrypt, or bypass particular Data FISes received at the cryptographic core, depending on whether those Data FISes include user data or control information. Pet. 38 (citing Ex. 1006 ¶¶ 166–68)*; see also id.* at 48–51 (addressing "bypass" limitations in claims 16, 17, and 19).

Patent Owner counters that that "the proposed combination of Sullivan and the SATA Specification fails to teach or suggest handling individual Data FISes differently than others." PO Resp. 47 (citing Ex. 2061 ¶¶ 81–116). This is essentially the same argument that Patent Owner presented with respect to claim 1, and it is not persuasive for the reasons discussed above.

Patent Owner further argues that Sullivan's filter embodiment teaches away from the "bypass" limitations because Sullivan's filter module "permits only two operations for packets that reach the cryptographic module: they are passed to the cryptographic module and encrypted, or they are rejected and filtered out." PO Resp. 47 (citing Ex. 2061 ¶¶ 104–05, 122). Thus, according to Patent Owner, Sullivan teaches only encrypting, decrypting, or rejecting packets, and does not teach bypassing cryptographic processing, as the "bypass" limitations require. *See id.* at 47–48.

We disagree that Sullivan's description of the filter module teaches away from causing certain FISes to bypass the cryptographic engine. Sullivan teaches that the filter module may be "configured to pass only a

any one of encrypting, decrypting, or bypassing (*see* Tr. 106:23–108:13), the parties appear to be in agreement that these limitations require that the controller is capable of instructing the cryptographic engine to bypass an FIS. Pet. 37–38; PO Resp. 45–46.

predetermined allowed set of commands, status and other information or categories of information." Ex. 1002 ¶ 55. Sullivan teaches that "[t]ypical allowed commands will be read, write, and other commands associated with data or memory access and storage." Ex. 1002 ¶ 56. Dr. Long and Dr. Conte agree that information that is allowed by Sullivan's filter is transmitted to the cryptographic core for encryption or decryption. *See* Ex. 1006 ¶ 114; Ex. 2061 ¶ 76.

Sullivan further teaches that, "[a]lternatively or additionally, the filter module may include logic to reject a predetermined set of information or categories of information, e.g. to reject certain types of data, address pointers, and so on." Ex. 1002 ¶ 55.[4] Based on this disclosure, Patent Owner contends that Sullivan's filter only permits two outcomes: (1) passing packets to the cryptographic module for encryption; or (2) rejecting them. PO Resp. 47 (citing Ex. 2061 ¶ 122).

However, because Sullivan describes the rejection feature as alternative or additional, we find Dr. Long's description of how a skilled artisan would have understood these teachings to be more credible. Dr. Long testifies that Sullivan's paragraph 55 "reminds us there's a number of ways to do this, look-up table, formula logic, whatever. It discloses the idea of you can pass some subset of commands to the encryption unit, and you can block other set of commands. It's silent on the intersection of those two sets." Ex. 2060, 74:3–8. Elaborating further, Dr. Long testifies:

[4] Sullivan does not state expressly what becomes of the information that is rejected. Dr. Conte testifies that it is "rejected and filtered out." Ex. 2061 ¶ 122. Dr. Long appears to be in agreement that information blocked by the rejection feature is not processed further. *See* Ex. 2060, 74:17–18 (testifying that "[t]here is a set of things that are blocked, which means they don't go anywhere").

> There's a set of things that are passed to the encryption unit. There is a set of things that are blocked, which means they don't go anywhere. And a person of ordinary skill in the art would think this through, but there could be things that are in neither set.

Id. at 74:16–21. In other words, Sullivan's description of the filter module leaves open the possibility that some of the information will be neither passed for encryption nor rejected and discarded. Thus, Sullivan's description of the filter module does not criticize, discredit, or otherwise discourage a skilled artisan from causing certain FISes to bypass the cryptographic engine.

Moreover, we agree with Petitioner that the bypassing limitations would have been obvious to a skilled artisan implementing Sullivan's teachings in view of SATA Standard. As discussed above with respect to claim 1, we agree with Petitioner that Sullivan teaches that control information should not be encrypted or decrypted. For example, Sullivan's claim 9 describes "transmitting the encrypted data with the associated control information to the second device, where the associated control information is transmitted in an unencrypted form." Ex. 1002, claim 9; *see* Reply 19. We find persuasive Dr. Long's testimony that a skilled artisan would have understood that in SATA, user data is transmitted as the payloads of Data FISes, but that Data FISes may also contain control information. Ex. 1006 ¶ 167. We further agree with Dr. Long that it would have been obvious, based on the teachings of Sullivan and SATA Standard, to encrypt, decrypt, or bypass the Data FIS received at the cryptographic engine, depending on whether those Data FISes included user data or control information. *Id.*

Based on the record before us, we are persuaded that Petitioner presents sufficient evidence to support a finding that the combination of Sullivan and SATA Standard renders obvious the "bypass" limitations of claims 5, 16, 17, and 19. Accordingly, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claim 5 would have been obvious over the combination of Sullivan and SATA Standard.[5]

5. Command Categories in Claims 7 and 9

Dependent claims 7 and 9 recite specific commands that are included in the predefined category of command set. *See* Ex. 1001, 13:45–50, 13:62–67. Petitioner argues that the commands recited in claims 7 and 9 are copied from SATA Standard, and that a skilled artisan would know that these commands are used for reading or writing user data. Pet. 39 (citing Ex. 1003, 250, 253; Ex. 1006 ¶ 171), *id.* at 43 (citing Ex. 1003, 252, 254; Ex. 1006, ¶¶ 176–77).

Patent Owner argues that SATA Standard does not group commands by whether they are read or write commands and, therefore, it does not teach the particular command sets of claims 7 and 9. PO Resp. 49 (citing Ex. 2061 ¶¶ 38–39, 126–27). Patent Owner further argues that Sullivan's teaching to pass for encryption "commands associated with data or memory access and storage" would have led skilled artisans to include commands that should not be cryptographically processed, such as SMART READ LOG. *See id.* at 50 (citing Ex. 2061 ¶ 128).

Patent Owner's arguments are not persuasive. It is undisputed that the commands recited in claims 7 and 9 appear in SATA Standard. *See*

[5] Patent Owner presents additional arguments regarding claims 16, 17, and 19, which are discussed below. Our conclusion regarding these claims is, therefore, provided below.

Ex. 1003, 250–254. Dr. Long testifies that a skilled artisan would have appreciated that the recited commands cause the transmission of user data. Ex. 1006 ¶¶ 171, 177.[6] We agree with Petitioner that "including these commands as part of the 'pre-defined category of command set' would have been obvious . . . in order to achieve Sullivan's goal of encrypting and decrypting the user data transferred in-line between the computer and the storage device." Reply 21 (citing Ex. 1006 ¶¶ 171, 176). Patent Owner's argument based on Sullivan is unpersuasive because it is premised on the proposition that a skilled artisan would have understood "other commands associated with data or memory access and storage" to include *any* command that happens to include the word "read," even when doing so would result in the encryption of control information, which runs counter to Sullivan's other teachings. *See* Ex. 1002 ¶ 56.

Based on the record before us, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claims 7 and 9 would have been obvious over the combination of Sullivan and SATA Standard.

6. Layers in Claims 16–19 and 28–32

Each of dependent claims 16–19 and 28–32 specify operations taking place at a certain SATA layer in the protocol stack.

Claims 16 and 17 recite an FIS type detector "configured to determine the FIS decoded at said Link layer" responsive to the type field having certain values. Ex. 1001, 14:21–32. Petitioner asserts that SATA Standard

[6] Furthermore, as discussed above with respect to claim 1, to the extent a skilled artisan was not already familiar with a particular command in SATA Standard, it would have been routine engineering work to consult the ATA specification to determine whether the command results in the transmission of user data.

specifies that the Link layer decodes received FISes. Pet. 48 (citing Ex. 1003, 129; Ex. 1006 ¶¶ 186, 188). The cited portion of SATA Standard supports Petitioner's assertions, insofar as it describes that when a frame is received from the Physical layer, the Link layer provides several services, including "decod[ing] the encoded 8b/10b character stream into aligned Dwords of data." Ex. 1003, 129. Relying on the testimony of Dr. Conte, Patent Owner counters that "the Link layer does not teach a FIS type detector as '[t]he Link layer is agnostic as to the content of the Frames it transports.'" PO Resp. 52 (quoting Ex. 2061 ¶ 32). Patent Owner's argument is not persuasive because it does not address specifically Petitioner's evidence summarized above. We note that the cited portion of Dr. Conte's declaration is providing background on SATA Standard, not addressing claims 16 or 17, much less Dr. Long's analysis of those claims.

Claims 18 and 19 require an ATA command filter for examining a command field of a Register-Host to Device FIS at the Transport layer. Ex. 1001, 14:33–44. Petitioner asserts that SATA Standard specifies that the Transport layer examines the contents of a Register-Host to Device FIS. Pet. 50 (citing Ex. 1003, 184–87, 231, 240–41; Ex. 1006 ¶ 190). We note that in describing the Transport layer, the cited portion of SATA Standard teaches that when a FIS is received from the Link layer, the Transport layer provides several services, including "determining FIS type." Ex. 1003, 184.

Claims 28–32 recite an ATA command filter for examining a command field of a FIS at the Link layer. Ex. 1001, 15:16–50. With respect to claims 28–32, Petitioner contends that it would have been obvious to a skilled artisan to place the recited function at the Link layer in order to reduce latency time. Pet. 57 (citing Ex. 1006 ¶¶ 197, 205). Specifically, relying on the testimony of Dr. Long, Petitioner asserts that examining the command field "at the Link layer instead of the Transport layer would achieve the predictable result of reducing latency time, for example, by identifying and distinguishing allowed commands from non-allowed commands without further processing by the Transport layer." *Id.* (citing Ex. 1006 ¶ 205).

With respect to claims 18, 19, and 28–32, Patent Owner argues that the prior art does not disclose accessing ATA commands at anything other than the Application layer, and that SATA Standard teaches that both the Link and Transport layers are unaware of the contents of a given FIS. PO Resp. 52 (citing Ex. 2061 ¶¶ 32–33). As with claims 16 and 17, Patent Owner's rebuttal is unpersuasive because it does not address Petitioner's evidence and arguments regarding claims 18, 19, and 28–32 summarized above.

Based on the record before us, we conclude that Petitioner has demonstrated by a preponderance of the evidence that claims 16–19 and 28–32 would have been obvious over the combination of Sullivan and SATA Standard.

E. Secondary Considerations

Patent Owner argues that secondary considerations in the form of industry praise, commercial success, copying, and licensing establish the nonobviousness of claims 1–32. PO Resp. 53–60.

Secondary considerations, when present, must always be considered as part of an obviousness inquiry. *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling USA, Inc.*, 699 F.3d 1340, 1349 (Fed. Cir. 2012). Factual inquiries for an obviousness determination include secondary considerations based on evaluation and crediting of objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). Notwithstanding what the teachings of the prior art would have suggested to one with ordinary skill in the art at the time of the patent's invention, the totality of the evidence submitted, including objective evidence of nonobviousness, may lead to a conclusion that the challenged claims would not have been obvious to one with ordinary skill in the art. *In re Piasecki*, 745 F.2d 1468, 1471–72 (Fed. Cir. 1984). Secondary considerations may include any of the following: long-felt but unsolved need, failure of others, unexpected results, commercial success, copying, licensing, and praise. *See Graham*, 383 U.S. at 17–18; *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007).

To be accorded substantial weight, there must be a nexus between the merits of the claimed invention and the evidence of secondary considerations. *In re GPAC Inc.*, 57 F.3d 1573, 1580 (Fed. Cir. 1995). "Nexus" is a legally and factually sufficient connection between the objective evidence and the claimed invention, such that the objective evidence should be considered in determining nonobviousness. *Demaco Corp. v. F. Von Langsdorff Licensing Ltd.*, 851 F.2d 1387, 1392 (Fed. Cir. 1988). The burden of showing that there is a nexus lies with the Patent Owner. *Id.*; *see In re Paulsen*, 30 F.3d 1475, 1482 (Fed. Cir. 1994).

1. Industry Praise

Patent Owner argues that its SATA-to-SATA X-Wall MX, and SATA-to-USB X-Wall FX products embody the claimed invention of the '057 patent, and have generated industry praise. PO Resp. 54–55 (citing Ex. 2046). We have reviewed the materials and find that Patent Owner has not established a sufficient nexus between the claimed cryptographic apparatus and the alleged industry praise of Patent Owner's products.

Patent Owner asserts that:

> Rocstor, a provider of fast, high-capacity data storage and encryption security solutions, describes Enova as "a leading ASIC design engineering company focused on bringing innovative encryption security solutions to market" and praises "Enova's leading-edge hardware based encryption products address the increasing requirement for privacy and confidentiality, satisfying the growing demand for maximum security."

Id. at 55 (citing Ex. 2018, 1). Although Exhibit 2018 discusses general features of Patent Owner's X-Wall products, Patent Owner does not identify any praise due to specific elements that are recited in the challenged claims. *See* PO Resp. 55; Ex. 2018.

Patent Owner also asserts that its products embodying the invention of the '057 patent have received industry awards. PO Resp. 55. Patent Owner asserts that its X-Wall MX product was awarded a 2012 Business World Golden Bridge Award in the Encryption Solutions Innovations category. *Id*.(citing Exs. 2020, 2038, 2039).[7] Exhibit 2020 only lists X-Wall MX without any discussion or description of X-Wall MX. Ex. 2020, 6. Further, Patent Owner does not provide any analysis explaining how its products embody any of the challenged claims of the '057 patent. *See* Tr. 62:10–64:6. Consequently, we are unable to determine whether the X-Wall product includes features recited in these challenged claims.

[7] Exhibits 2038 and 2039 appear to be copies of product literature for the X-Wall. Patent Owner does not cite to any particular portion of these lengthy exhibits, or explain how they are germane to its secondary consideration argument. *See* PO Resp. 55.

Accordingly, Patent Owner has not established a sufficient nexus between the merits of the claimed invention and industry praise of Patent Owner's products.

2. Commercial Success

As evidence of commercial success, Patent Owner relies on its previous business relationship with Petitioner and Petitioner's alleged praise and advertisement of Patent Owner's encryption devices. PO Resp. 55–57. We are not persuaded Patent Owner has established a sufficient nexus between the merits of the claimed invention and either Patent Owner's own products or Petitioner's products.

Patent Owner argues that Petitioner sought out Patent Owner's assistance to bring hardware encryption products to market. PO Resp. 56. Patent Owner further asserts that Petitioner purchased Patent Owner's X-Wall products and used them in Petitioner's hard disk drives, including Petitioner's Momentus drive. *Id.* (citing Ex. 2027 ¶¶ 15–17). According to Patent Owner, by using Patent Owner's products, Petitioner touted and advertised the advantages of hardware-based full disk encryption and transparent encryption. *Id.* at 56–57. Patent Owner further asserts that Petitioner extended the '057 patent's hardware encryption technology to Petitioner's BlackArmor product, and that "Seagate's chief technologist, Dr. Robert Thibadeau, praised the patented hardware encryption technology Enova provided to Seagate." *Id.* (citing Ex. 2005, 3–6)).

Patent Owner's assertions are unpersuasive to the extent that they are based on unsubstantiated allegations made in its own Complaint, from the related district court proceeding between the parties, which Petitioner denied in a responsive Answer. *See* PO Resp. 56 (citing Ex. 2027). For example, Patent Owner argues that the sales and awards of Petitioner's "BlackArmor" product support the nonobviousness of the '057 patent. *Id.* at 57–58 (citing Ex. 2009, 1; Ex. 2021, 1; Ex. 2027 ¶ 26). Presumably, Patent Owner's assertion is based on the allegation that Petitioner's BlackArmor product infringes the '057 patent. Ex. 2005 ¶ 40. Petitioner disputes Patent Owner's allegations (*id.*) and Patent Owner has not established that the BlackArmor product infringes the '057 patent or incorporates any claimed elements of the '057 patent.

"Evidence of commercial success, or other secondary considerations, is only significant if there is a nexus between the claimed invention and the commercial success." *Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1311–12 (Fed. Cir. 2006). To show how commercial success supports nonobviousness, Patent Owner must prove that the sales were a direct result of the unique characteristics of the invention, and not a result of economic and commercial factors unrelated to the quality of the patented subject matter. *In re Applied Materials, Inc.*, 692 F.3d 1289, 1299–1300 (Fed. Cir. 2012). In addition, "if the commercial success is due to an unclaimed feature of the device," or "if the feature that creates the commercial success was known in the prior art, the success is not pertinent." *Ormco*, 463 F.3d at 1312; *see also In re Kao*, 639 F.3d 1057, 1070 (Fed. Cir. 2011) (requiring a determination of "whether the commercial success of the embodying product resulted from the merits of the claimed invention as opposed to the prior art or other extrinsic factors").

Here, Patent Owner fails to provide sufficient proof of such a relationship between any alleged sales and the unique characteristics of the invention embodied in the challenged claims. First, Patent Owner has not established that Petitioner's products include features claimed in the '057 patent. PO Resp. 56–57. Patent Owner simply relies on allegations made in the Complaint of the related district court proceeding, which, as we explained above, Petitioner has denied. *Id.; see also* Ex. 2027 ¶ 40 (denying infringement of the '057 patent).

Moreover, even if Petitioner's product sales are considered in the context of commercial success, "evidence related solely to the number of units sold provides a very weak showing of commercial success, if any." *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996). According to the Federal Circuit, "the more probative evidence of commercial success relates to whether the sales represent 'a substantial quantity in th[e] market.'" *Applied Materials*, 692 F.3d at 1300 (quoting *Huang*, 100 F.3d at 140). Patent Owner offers no evidence of the size of the market to which to compare Petitioner's sales. Accordingly, we are not persuaded that Patent Owner's alleged objective indicia of commercial success shows non-obviousness.

3. Copying and Licensing

Patent Owner further argues that copying and licensing of the '057 patent by others is objective indicia of non-obviousness. Specifically, Patent Owner argues that Initio Corporation ("Initio") marketed and sold infringing products incorporating the claimed invention of the '057 patent to major hard drive manufactures. PO Resp. 58–59 (citing Ex. 2032; Ex. 2059). Patent Owner contends the resolution of *Enova v. WD* "confirms Initio's infringement of the '057 patent" because "Initio admitted in a consent judgment that its products practice the '057 patent and further began marking its products with the '057 patent number." *Id.* at 58 (citing Ex. 2059, 2). Patent Owner additionally argues that Western Digital and

Buffalo, Inc., each incorporated Initio encryption circuits in their hard drives, and that both parties entered agreements with Patent Owner to resolve their disputes in *Enova v. WD*. *Id.* at 59 (citing Ex. 2024; Ex. 2042–45). Patent Owner adds that both Initio and Western Digital license the ’057 patent from Patent Owner.

With respect to Patent Owner’s reliance on Initio’s consent judgement in *Enova v. WD,* it is not sufficient that a product is within the scope of a claim in order for objective evidence of nonobviousness tied to that product to be given substantial weight. Like other types of objective evidence, evidence of copying must be shown to have nexus. *Wm. Wrigley Jr. Co. v. Cadbury Adams USA LLC*, 683 F.3d 1356, 1364 (Fed. Cir. 2012). Moreover, a showing of copying is only equivocal evidence of nonobviousness in the absence of more compelling objective indicia of other secondary considerations. *Ecolochem, Inc. v. S. Cal. Edison Co.,* 227 F.3d 1361, 1380 (Fed. Cir. 2000). Copying could result from lack of concern about patent property, contempt for the patent, or accepted practices in the industry, among others. *Cable Elec. Prods., Inc. v. Genmark, Inc.*, 770 F.2d 1015, 1028 (Fed. Cir. 1985), *overruled on other grounds by Midwest Indus., Inc. v. Karavan Trailers, Inc.,* 175 F.3d 1356, 1359 (Fed. Cir. 1999).

We also are not persuaded by Patent Owner’s arguments regarding licensing and settlement. “Licenses taken under the patent in suit may constitute evidence of nonobviousness; however, only little weight can be attributed to such evidence if the patentee does not demonstrate ‘a nexus between the merits of the invention and the licenses of record.’” *GPAC*, 57 F.3d at 1580 (quoting *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1539 (Fed. Cir. 1983)). Here, Patent Owner has not established that the licenses arose out of recognition and acceptance of the subject matter claimed in the ’057 patent. *See id.* Indeed, the version of the licenses that Patent Owner relies on in this proceeding are almost entirely redacted. Because we cannot verify Patent Owner’s assertions regarding these agreements, we find that these agreements do not provide objective evidence of nonobviousness.

4. Summary

On balance, we determine that Petitioner’s evidence of obviousness outweighs the evidence of secondary considerations of nonobviousness submitted by Patent Owner.

F. Patent Owner’s Motion to Seal

Patent Owner filed a Motion to Seal Exhibits 2042, 2043, and 2044 under 37 C.F.R. § 42.54. Paper 25 (“Mot. to Seal”). In its Motion, Patent Owner asserts that the redacted exhibits are “confidential” agreements reached between the Patent Owner and third parties Initio, Western Digital, and Buffalo, Inc., each of which is not involved in this proceeding. Mot. to Seal 1–2. With its Motion to Seal, Patent Owner filed confidential redacted versions of Exhibits 2042, 2043, and 2044, but did not file confidential un-redacted copies. Patent Owner indicated that it intended to file un-redacted versions of the agreements, but had not received the consent of the third parties to do so. Mot. to Seal 2.

The standard for granting a motion to seal is “for good cause.” 37 C.F.R. § 42.54. Patent Owner, as the moving party, has the burden of proof in showing entitlement to the requested relief. 37 C.F.R. § 42.20(c). This burden includes showing that the information sought to be sealed is truly confidential, and that such confidentiality outweighs the strong public policy interest in having an open record in *inter partes* reviews.

In reviewing the "confidential" version of these exhibits, we note that each exhibit has been heavily redacted, leaving only a handful of lines per each exhibit. These un-redacted portions do not provide sufficient detail to verify the contents of these exhibits. Thus, we cannot confirm Patent Owner's assertions regarding the confidentiality of these exhibits, nor can we grant Patent Owner's Motion to Seal for good cause. Accordingly, we deny Patent Owner's Motion to Seal Exhibits 2042, 2043, and 2044.

Additionally, Patent Owner has submitted a revised proposed protective order (Ex. 2049) that reflects the terms of a protective order entered in the parties' co-pending district court proceeding. Mot. to Seal 2. Patent Owner represents that it has conferred with Petitioner regarding the terms of the proposed protective order; however, no agreement has been reached. *Id.* at 3.

We note that the Office Patent Trial Practice Guide states the following concerning protective orders:

> (a) Purpose. This document provides guidance on the procedures for filing of motions to seal and the entry of protective orders in proceedings before the Board. The protective order governs the protection of confidential information contained in documents, discovery, or testimony adduced, exchanged, or filed with the Board. The parties are encouraged to agree on the entry of a stipulated protective order. *Absent such agreement, the default standing protective order will be automatically entered.*

Office Patent Trial Practice Guide, 77 Fed. Reg. 48756, 48769 (Aug. 14, 2012) (App'x B (emphasis added)). As we cannot ascertain that the contents of the redacted Exhibits 2042, 2043, and 2044 constitute the Patent Owner's confidential information, we do not grant Patent Owner's request to enter its proposed protective order. We do, however, enter the default Protective Order provided in Appendix B of the Trial Practice Guide.

III. CONCLUSION

We conclude Petitioner has shown by a preponderance of the evidence that claims 1–32 of the '057 patent are unpatentable under 35 U.S.C. § 103 over Sullivan and SATA Standard.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–32 of the '057 patent are held unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Seal is *denied*;

FURTHER ORDERED that the Board's default Protective Order appearing in the Office Trial Practice Guide, 77 Fed. Reg. 48,756, 48,769–71 (Aug. 14, 2012), is hereby *entered* in this proceeding; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to this proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Richard Marsh
Richard.marsh@faegrebd.com

Elizabeth Cowan Wright
Elizabeth.cowanwright@faegrebd.com

David Gross
David.gross@faegrebd.com

Calvin Litsey
Calvin.litsey@faegrebd.com

PATENT OWNER:

Ajeet Pai
apai@velaw.com

Seth A. Linder
slindner@velaw.com