

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Petitioner,

v.

DIGITAL DOORS, INC.,
Patent Owner.

IPR2023-00970
Patent 7,552,482 B2

Before THU A. DANG, THOMAS L. GIANNETTI, and
ELIZABETH M. ROESEL, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. *Background*

International Business Machines Corporation (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1, 5, 25, 26, 30, and 50 of U.S. Patent No. 7,552,482 B2 (Ex. 1001, “the ’482 patent”). Paper 2 (“Pet.”). Digital Doors, Inc. (“Patent Owner”) filed a Preliminary Response to the Petition. Paper 6 (“Prelim. Resp.”).

We have jurisdiction under 35 U.S.C. § 314 (2018) and 37 C.F.R. § 42.4(a) (2023). Applying the standard set forth in 35 U.S.C. § 314(a), we may not institute an *inter partes* review (also “IPR”) unless the information presented in the petition “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” However, institution of *inter partes* review is discretionary. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1367 (Fed. Cir. 2016) (“[T]he PTO is permitted, but never compelled, to institute an IPR proceeding.”). For the reasons stated below, we exercise our discretion not to institute an *inter partes* review.

B. *Related Proceedings*

The parties indicate that the ’482 patent is the subject of *Digital Doors, Inc. v. International Business Machines Corporation.*, Case No. 2:22-cv-00457 (E.D. Tex.) (“Texas Litigation”). Pet. 83; Paper 3, 1.

C. *The ’482 Patent (Ex. 1001)*

The ’482 patent, titled “Data Security System and Method,” issued on June 23, 2009, discloses a method for securing data that includes filtering and extracting sensitive content by security level and separately storing the security sensitive content in remote extract stores. Ex. 1001, codes (45), (54), (57). Remainder data is stored locally or remotely. *Id.* at code (57).

According to the method, encryption is utilized to enhance security (including transfers of data, files and maps), and full or partial reconstruction of the data is permitted only in the presence of a predetermined security clearance. *Id.* Figures 1A and 1B of the '482 patent illustrate this method and are reproduced below.

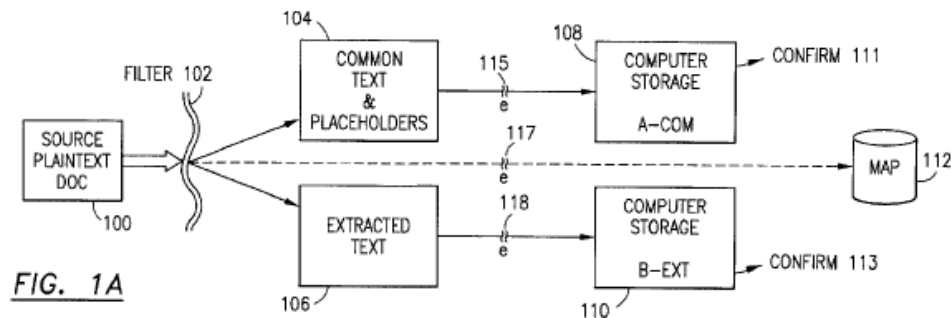


Figure 1A illustrates the basic processes for establishing a secure storage of information, generally identified as “data.” *Id.* at 14:33–35. In the '482 patent, the term “data” includes “any data object, e.g., text, images, icons, moving images, multiple images, data representing sound, video, electronic streams of information, etc. Sound bites, data objects and video images may also be extracted as ‘data.’” *Id.* at 14:35–37.

As shown in Figure 1A, in operation, source document 100 or “plaintext” is passed through filter 102, which separates out common text or remainder data 104 from uncommon text, words, characters, or icons. *Id.* at 14:37–41. The security sensitive words, characters, or icons are separated there from remainder or common text 104 as extracted text 106. *Id.* at 14:41–43. Filter 102 may use a dictionary such that words present in the dictionary (common words) are separated from source plaintext document 100 and placed into remainder document or common data file 104. *Id.* at 14:48–52. The uncommon words (extracted-security sensitive words), not found in the dictionary, would be placed in an extracted text or extracted

data file 106. *Id.* at 14:52–54. The common text or remainder data would be stored in remainder data file 104. *Id.* at 14:59–60. In the illustrated embodiment, remainder data file 104 also includes place holders, which enables the extracted data to be easily inserted or set back into the remainder data file. *Id.* at 14:60–63.

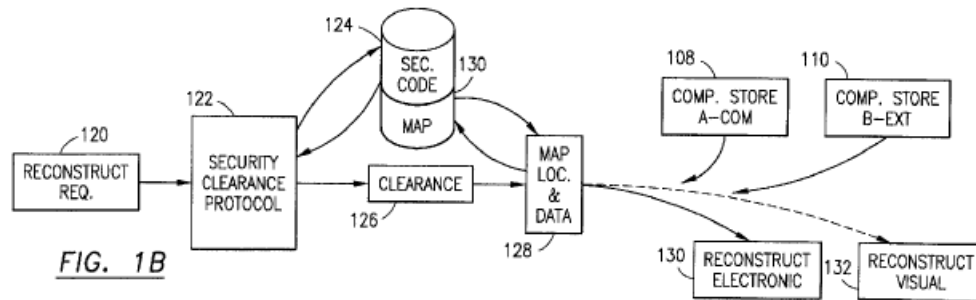


Figure 1B illustrates the major features of a reconstruction routine or system. *Id.* at 15:65–66. As shown in Figure 1B, in operation, the user inputs reconstruction request 120, and the system executes security clearance protocol routine 122 in order to determine whether the user has the proper security clearance. *Id.* at 15:66–3. In particular, the security code input by the user is checked against security code database or list 124. *Id.* at 16:8–10. Clearance is provided in step 126, and the location of a map identifying the location of remainder data A-com 108 and extraction data B-ext 110 is provided to the user's computer in step 128. *Id.* at 16:10–13. As shown in Figure 1B, the storage segments are A-com 108 and B-ext 110, and the common or remainder data from A-com 108 is downloaded or transferred or made available to the user's computer as shown at the output of map location and data step 128. *Id.* at 16:16–19. Typically, the extracted or security sensitive data from B-ext 110 also is downloaded. *Id.* at 16:19–20. The data is then reconstructed as a complete electronic document in function 130 or as a visual reconstruction in step 132. *Id.*

at 16:21–23.

D. Challenged Claims

Of the challenged claims (1, 5, 25, 26, 30, and 50), claims 1 and 26 are the independent claims. Claims 5 and 25 depend from claim 1, and claims 30 and 50 depend from claim 26. Independent claim 1 is illustrative and reproduced below:

1. A method of securing data on a personal computer having security sensitive content represented by one or more security sensitive words, characters, images or data objects therein, said security sensitive content having a plurality of security levels, each security level having an associated security clearance, the method of securing data deployed in a distributed computer system with a plurality of other computers and a plurality of extract data stores for respective ones of said plurality of security levels, said personal computer, said other computers and said extract data stores operatively connected together over a communications network comprising:

accepting data input which includes security sensitive content via said personal computer;

extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data;

storing said extracted data for each corresponding security level in the respective extract store and storing said remainder data in at least one of said personal computer and other computers; and,

permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores for corresponding security levels with said associated security clearances.

Ex. 1001, 24:19–44.

E. Asserted Grounds of Unpatentability

Petitioner contends that claims 1, 5, 25, 26, 30, and 50 of the '482 patent are unpatentable based on the following grounds (Pet. 7):

Claim(s) Challenged	35 U.S.C. §¹	Reference(s)/Basis
1, 5, 25, 26, 30, 50	103	Merenda ²
1, 5, 25, 26, 30, 50	103	Bossemeyer ³
1, 5, 25, 26, 30, 50	103	Bossemeyer, Merenda

Petitioner also relies on a Declaration from Erez Zadok, Ph.D. (Ex. 1003). Patent Owner relies on a Declaration of William C. Easttom II, Ph.D. (Ex. 2004).

II. ANALYSIS - DISCRETION TO DENY INSTITUTION UNDER § 314(A)

Institution of an *inter partes* review is discretionary. *See* 35 U.S.C. § 314(a) (authorizing institution of an *inter partes* review under particular circumstances, but not requiring institution under any circumstances); *Cuozzo Speed Techs., LLC v. Lee*, 579 U.S. 261, 273 (2016) (“[T]he agency’s decision to deny a petition is a matter committed to the Patent Office’s discretion.”); *SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1356 (2018)

¹ The relevant sections of the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, took effect on March 16, 2013. The '344 patent claims priority to applications with filing dates before this date. *See* Ex. 1001, codes (22), (62). For the purposes of this Decision, pre-AIA statutes apply.

² Merenda et al., US 2004/0148290 A1, published July 29, 2004 (Ex. 1006).

³ Bossemeyer et al., US 7,010,701 B1, issued March 7, 2006 (Ex. 1005).

(“[Section] 314(a) invests the Director with discretion on the question whether to institute review” (emphasis omitted)); *Harmonic*, 815 F.3d at 1367 (“[T]he PTO is permitted, but never compelled, to institute an IPR proceeding.”).

When determining whether to exercise discretion to deny institution in view of a parallel proceeding, we consider the following factors:

1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
2. proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision;
3. investment in the parallel proceeding by the court and the parties;
4. overlap between issues raised in the petition and in the parallel proceeding;
5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
6. other circumstances that impact the Board’s exercise of discretion, including the merits.

See Apple Inc. v. Fintiv, Inc., IPR2020 00019, Paper 11 at 6 (PTAB Mar. 20, 2020) (precedential) (“*Fintiv*”). “These factors relate to whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding.” *Id.* In evaluating the *Fintiv* factors, we take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review,” recognizing that “there is some overlap among these factors” and that “[s]ome facts may be relevant to more than one factor.” *Id.*

On June 21, 2022, the Director of the United States Patent and Trademark Office issued a Memorandum setting forth an “Interim Procedure for Discretionary Denials in AIA Post Grant Proceedings with Parallel District Court Litigation.” Exhibit 1015 (“Guidance Memo”). The

Guidance Memo states that “to benefit the patent system and the public good, the PTAB will not rely on the *Fintiv* factors to discretionarily deny institution in view of parallel district court litigation where a petition presents compelling evidence of unpatentability.” *Id.* at 2. “Compelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” *Id.* at 4.

Patent Owner argues that we should exercise our discretion under 35 U.S.C. § 314(a) and not institute trial. Prelim. Resp. 27–39. In particular, Patent Owner contends that: the district court is highly unlikely to grant a stay (*id.* at 32–33); trial may proceed before the Final Written Decision (*id.* at 33); the parties and the district court have invested substantial resources into the co-pending litigations (*id.* at 34); the parties “broadly make the *same* arguments using the *same* references as the Petition” with respect to the limitations found in the challenged claims (*id.* at 34–36); Petitioner and Defendants in the district court proceeding are the same party (*id.* at 36–37); and the Petition “falls well-short of the ‘compelling merits’ standard required to avoid a discretionary denial based on *Fintiv* Factors 1-5.” *Id.* at 37.

Petitioner argues that we should not deny institution because the *Fintiv* factors “weigh heavily against discretionary denial.” Pet. 84. In particular, Petitioner contends that “[i]t is highly unlikely that any of the parallel proceedings will proceed to trial before the projected final written decision date of January 2025 in this proceeding.” *Id.* Further, Petitioner contends that “the district courts . . . have not made any substantive rulings related to the ’649 patent” and points out that Petitioner “is not a defendant in any of the parallel cases.” *Id.* at 85. Petitioner then contends that the

Petition “presents compelling merits that the challenged claims are unpatentable.” *Id.*

In the analysis as set forth below, we first consider whether *Fintiv* factors 1–5 weigh in favor of denying institution, and, if so, we must also determine whether the Petition presents compelling merits. *See CommScope Technologies LLC v. Dali Wireless, Inc.*, IPR2022-01242, Paper 23 (PTAB Feb. 27, 2023) (precedential) (“*CommScope*”) (“In circumstances where . . . the Board’s analysis of *Fintiv* factors 1–5 favors denial of institution, the Board shall then assess compelling merits.”). For the reasons stated below, we exercise our discretion to deny institution in view of the parallel district court litigation.

A. Likelihood of a Stay

A district court stay of parallel litigation pending resolution of an *inter partes* review allays concerns about inefficiency and duplication of efforts, which strongly weighs against exercising the authority to deny institution. *Fintiv*, Paper 11 at 6.

Here, Petitioner’s motion to stay the district court litigation pending in the Eastern District of Texas was denied on July 24, 2023. Ex. 2007. In denying the stay, Magistrate Judge Payne stated that to prevail on a stay motion, “IBM needs to show that every asserted claim has a reasonable likelihood of being invalidated by the PTAB.” *Id.* at 5. Judge Payne continued that “[h]ere, the PTAB has not publicly determined that any asserted claim has a reasonable likelihood of being invalidated.” *Id.*

Patent Owner points out that there are 54 claims and seven patents involved in the district court proceeding, and that because the court has made it clear that it will not grant stay unless there is a showing that every

asserted claim has a reasonable likelihood of being invalidated, a stay is unlikely. Prelim. Resp. 63.

However, *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 12 (PTAB May 13, 2020) (informative), cautions against speculating whether the district court would grant a stay if one were requested. Accordingly, this factor is neutral.

B. Proximity of Trial Date to Projected Statutory Deadline

The projected statutory deadline for issuance of a final written decision in this proceeding is early January 2025, one year from the date of this Decision. Jury selection in the parallel district court litigation has been scheduled by Judge Gilstrap for August 19, 2024. *See* Ex. 1007, 1. As Patent Owner points out, trial is scheduled to begin before the statutory deadline for our final written decision. Prelim. Resp. 63–64.

We are not persuaded by Petitioner’s argument based on Petitioner’s median-time-to-trial data. Pet. 78–79. In particular, although Petitioner contends that the projected trial date is between June 2024 and December 2024 (*id.* at 79 (citing Ex. 1009, 1)), we agree with Patent Owner that the most recent (March 2023) median time-to-trial statistics for the Eastern District of Texas predict a trial date is June 2024, even earlier than the August 2024 trial date set by Judge Gilstrap. Prelim. Resp. 64 (citing Ex. 1009).⁴

⁴ The Guidance Memo approves the submission of the “most recent” median time-to-trial statistics for the district, among other evidence of projected trial dates. *See* Guidance Memo at 8–9 (“Parties may present evidence regarding the most recent statistics on median time-to-trial for civil actions in the district court in which the parallel litigation resides for the PTAB’s consideration.”) (footnote omitted).

Here, the evidence presented by the parties suggests that a trial in the parallel district court litigation is likely to occur prior to the due date of our final written decision if we were to institute an *inter partes* review. That is, based on the court’s scheduling order, trial would occur about five months before the statutory deadline. Further, based on the most recent (March 2023) median time-to-trial statistics for the Eastern District of Texas, trial would occur about seven months before the statutory deadline.

Because the evidence presented by the parties suggests that, by any measure, a trial in the parallel district court litigation is likely to occur before the due date of our final written decision if we were to institute an *inter partes* review, this factor favors exercising our discretion to deny the Petition.

C. Investment in the Parallel Proceeding

Regarding *Fintiv* factor 3, Patent Owner contends that “[t]he parties have expended substantial resources on the pending district court case in the eight months since this suit was filed.” Prelim. Resp. 64–65. According to Patent Owner, it has “prepared and served 1,067 pages of infringement contentions.” *Id.* at 65. Patent Owner asserts that IBM “drafted and served 10,171 pages of invalidity contentions,” wherein documents have been produced and there have been there have been “multiple” fact witness depositions and “multiple rounds of discovery requests and responses.” *Id.*

While the district court proceeding has already advanced well beyond the pleadings stage and discovery is underway, there is still much work to be done on the case, particularly as it relates to claim construction and invalidity. We find this factor is neutral.

D. Overlap of Issues

Regarding *Fintiv* factor 4, Patent Owner argues that the same two references, Bossemeyer and Merenda, were asserted in the district court proceedings, and thus, “institution of an IPR risks duplication of resources and conflicting outcomes.” Prelim. Resp. 65 (citing Ex. 2008).

Anticipating this argument, Petitioner stipulates that “if the IPR is instituted, Petitioner will not pursue the same grounds in the district court litigation.” Pet. 80 (citing *Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative) (“*Sand Revolution*”). However, according to Patent Owner, it is “insufficient to overcome [] concerns of duplicative efforts and conflicting outcomes based on the Board’s own current guidance on the *Fintiv* factors.” Prelim. Resp. 66 (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 18–19 (PTAB Dec. 1, 2020) (precedential as to § II.A) (“*Sotera*”). Patent Owner argues that the Board’s guidance “requires petitioners to stipulate that they will not ‘pursue in a parallel proceeding the same grounds **or any grounds that could have reasonably been raised before the [Board].**’” *Id.* (citing Ex. 1018, 3) (emphasis in original).

We agree with Patent Owner (Prelim. Resp. 66) that Petitioner’s stipulation is narrower than a *Sotera* stipulation, *i.e.*, a stipulation not to pursue in a parallel district court proceeding the same grounds as in the petition “or any grounds that could have reasonably been raised in the petition.” *See Guidance Memo* at 7, 9; *Sotera*, Paper 12 at 13–14, 18. However, Petitioner’s stipulation does reduce the overlap relating to the challenge presented in the Petition and “mitigates to some degree the concerns of duplicative efforts between the district court and the Board, as

well as concerns of potentially conflicting decisions.” *See Sand Revolution*, Paper 24 at 12. For these reasons, this factor weighs marginally against discretionary denial. *Id.*

E. Identity of Parties

Regarding *Fintiv* factor 5, Patent Owner asserts that this factor weighs in favor of denial because Petitioner and the Defendant in the district court proceeding are the same party. Prelim. Resp. 66. Petitioner does not dispute this fact, but remarks that it is “true of most Petitioners in IPR proceedings,” and should not be a basis for denying institution. Pet. 80.

Because Petitioner here is a defendant in the parallel district court litigation, this factor favors denial of institution under § 314(a). *See also Sotera*, Paper 12 at 19 (citing *Fintiv*, Paper 15 at 15; *Sand Revolution*, Paper 24 at 12–13).

F. Other Circumstances, Including the Merits

Under *CommScope*, if we determine that the other *Fintiv* factors favor discretionary denial, we must also consider whether the Petition presents compelling merits. *See CommScope*, Paper 23 at 4–5.

We take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review” when evaluating these factors. *Fintiv*, Paper 11 at 6. We have considered the circumstances and facts before us in view of *Fintiv* factors 1–5. As discussed above, factors 1 and 3 are neutral, factors 2 and 5 weigh in favor of discretionary denial of institution, and factor 4 weighs marginally against discretionary denial. We, therefore, conclude that the evidence of record on factors 1–5 favors exercising our discretion to deny institution of an *inter partes* review.

Accordingly, following *CommScope*, where, as here, our analysis of the first five *Fintiv* factors favors denial of institution. we address the merits of the Petition to determine whether the merits are compelling.

III. ANALYSIS – COMPELLING MERITS

A. Claim Construction

We construe each claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b) (2020). Under this standard, claim terms are generally given their plain and ordinary meaning as would have been understood by a person of ordinary skill in the art (“POSITA”) at the time of the invention and in the context of the entire patent disclosure. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (*en banc*).

On the record before us, we do not find it necessary to construe any term for purposes of this Decision. *See, e.g., Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that “only those terms need to be construed that are in controversy, and only to the extent necessary to resolve the controversy”))); *see also Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (applying *Vivid Techs.* in the context of an *inter partes* review).

B. Level of Ordinary Skill in the Art

Petitioner asserts that a POSITA would have “a bachelor’s degree in computer science, computer engineering, electrical engineering, or equivalent, and approximately two years of experience working in the field

of data storage systems and data security,” wherein “[l]ess professional experience can be substituted by additional education and vice versa.” Pet. 5 (citing Ex. 1003 ¶¶ 110–111).

Patent Owner does not contest Petitioner’s proposal or offer an alternative. On this record, we are persuaded that Petitioner’s proposal is consistent with the technology described in the Specification and the cited prior art. For purposes of this Decision, we adopt Petitioner’s proposed level of skill.

C. Obviousness of Claims 1, 5, 25, 26, 30, and 50

Petitioner contends that the challenged claims of the ’482 patent “cover methods for securing data by separating and securing sensitive portions of the data and then controlling access to the sensitive data based on security clearance,” wherein “[t]his Petition demonstrates that separating and securing sensitive data in a separate location was known.” Pet. 1–2. In particular, Petitioner contends that Merenda renders obvious claims 1, 5, 25, 26, 30, and 50. *Id.* at 14–36 (ground 1). Alternatively, Petitioner contends that Bossemeyer (ground 2) or Bossemeyer in view of Merenda (ground 3) renders obvious claims 1, 5, 25, 26, 30, and 50. *Id.* at 36–77.

In response, Patent Owner contends that Petitioner has failed to show that Merenda teaches or renders obvious every limitation of the challenged claims. Prelim. Resp. 39–49. Patent Owner also contends that Bossemeyer is not analogous art to the ’482 patent. *Id.* at 23–24. Patent Owner then contends that Petitioner has failed to show that Bossemeyer teaches or renders obvious every limitation of the challenged claims. *Id.* at 24–39. With respect to ground 3, Patent Owner further contends that a person of ordinary skill would not have found it obvious to combine Merenda with Bossemeyer. *Id.* at 49–61. We summarize the asserted prior art below.

1. Merenda (Ex. 1006)

Merenda, titled “Method, System and Program Product for Private Data Access or Use Based on related Public data,” discloses “allowing the viewer of a public data set to access related records in a private data set based upon a link which may be selectively provided to the viewer to authorize such access.” Ex. 1006, code (54), ¶ 2. Fundamental to the implementation of Merenda is “the notion that a set of data may be parsed into private and non-private elements.” *Id.* ¶ 23.

In one embodiment, data entered by a consumer into a Web form is separated into related records in a public and private data set. *Id.* ¶ 7. In this embodiment, the public records would be available without restriction for read access by a population of merchants. *Id.* The private records would be available only per the indication of the consumer to the merchant in the population. *Id.* The records may be logically linked by the inclusion of a common key value into each of these records to indicate, for example, that these records emanated from a common source. *Id.* Figure 2 of Merenda depicts the separation of public and private data, and is reproduced below.

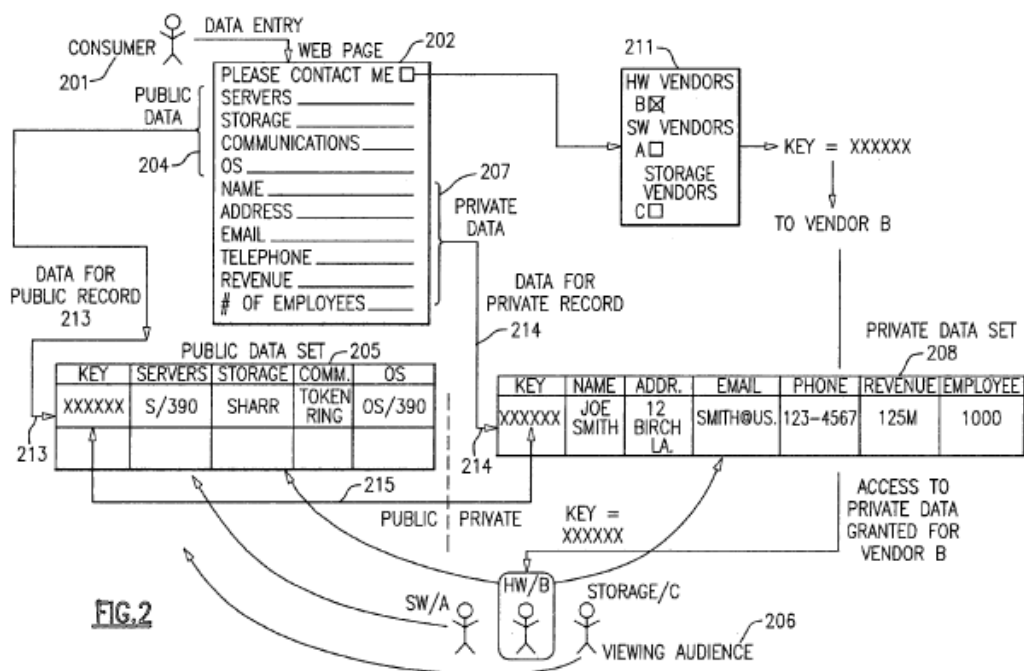


Figure 2 depicts the separation of public and private data into their respective data sets and consumer designated access for specified members of the viewing population to the private data set. *Id.* ¶ 16.

In an alternative embodiment, upon designation by the consumer, the various logically linked records in public and private tables for that consumer may be collected and assembled into an output Web page. *Id.* ¶ 10. The Web page is provided at a uniform resource locator (URL) which has been coded with the common key value linking the related records or with another pass code. *Id.* The merchant for whom access has been indicated is provided, either via e-mail or otherwise, with a hyperlink to the coded URL thereby enabling the selected merchant to access both the public and private data. *Id.* Figure 3 of Merenda depicts providing the combined public and private data to a merchant in the form of a customized Web page.

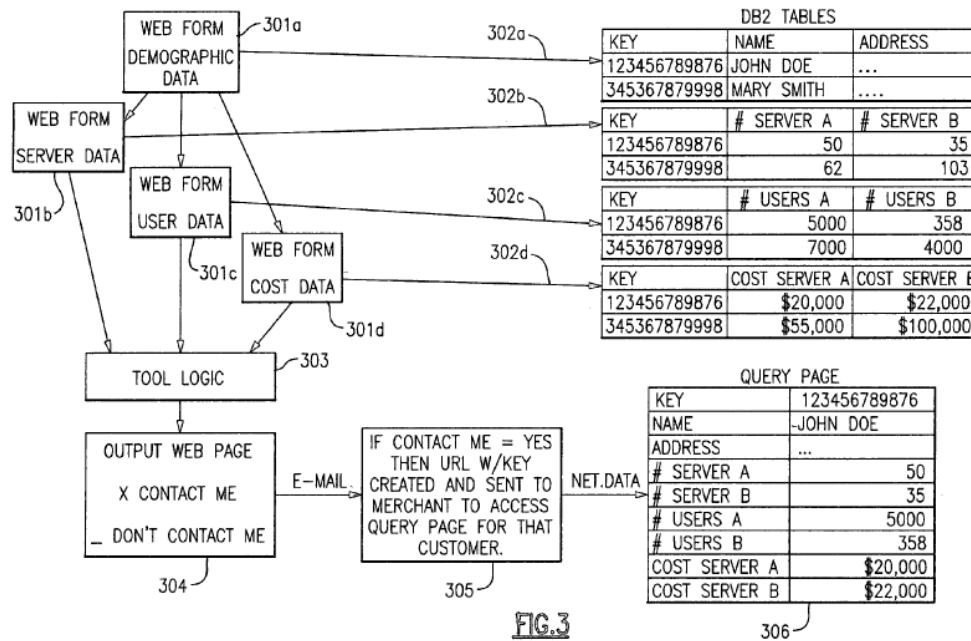


Figure 3 depicts the combined public and private data being provided to a merchant in the form of a customized Web page using a specific key inserted into the URL for the Web page. *Id.* ¶ 17.

1. Bossemeyer (Ex. 1005)

Bossemeyer, entitled “Network Arrangement for Smart Card Applications,” relates to “a network arrangement to provide access to an architecture that supports a variety of advanced smart card applications.” Ex. 1005, code (54), 1:8–11. In particular, Bossemeyer “describes a network arrangement which is readily accessible from different types of smart card terminals supporting various smart card applications.” *Id.* at 1:44–47. “The network connections are facilitated by the present telephone network or an interconnected network of computers such as the Internet.” *Id.* at 1:47–49. Bossemeyer’s network arrangement also includes “a centralized server architecture, [where] data related to an individual can be accessed by an individual smart card, predefined groups of smart card users, or the general public.” *Id.* at 1:49–52.

This arrangement is depicted in Figure 1 of Bossemeyer, which is reproduced below.

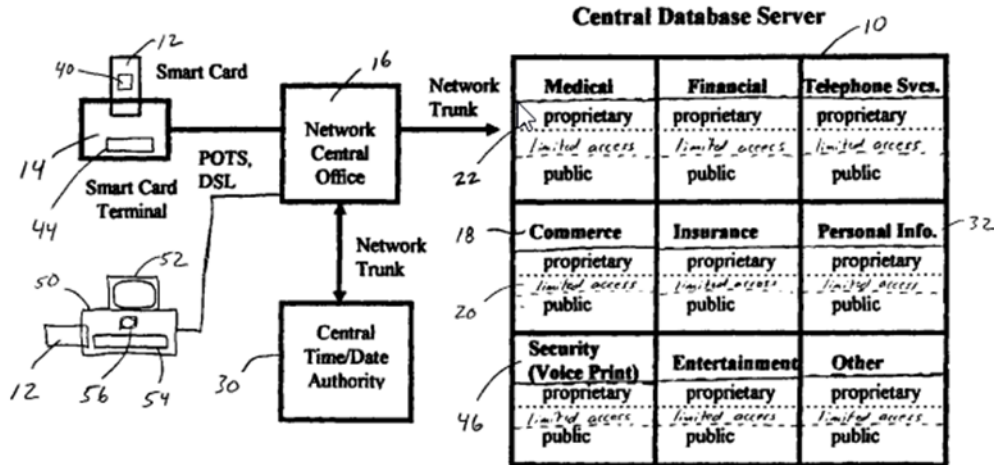


Figure 1

Figure 1 of Bossemeyer depicts smart card 12 and smart card terminal 14 connected to central database server 10 through telephone system central office 16. *Id.* at 2:9–12. Central database server 10 includes partitioned memory, as well as a microprocessor for processing data received from and transmitted to smart card terminal 14. *Id.* at 2:13–16. The information is stored in the partitioned memory by category (medical, financial, etc.) as well as level of security (unrestricted, or public limited access, restricted). *Id.* at 2:20–22. Private or proprietary information is partitioned such that the owner of the information has control over how the information is transferred and used. *Id.* at 2:28–30. This is illustrated in Figure 3, reproduced below.

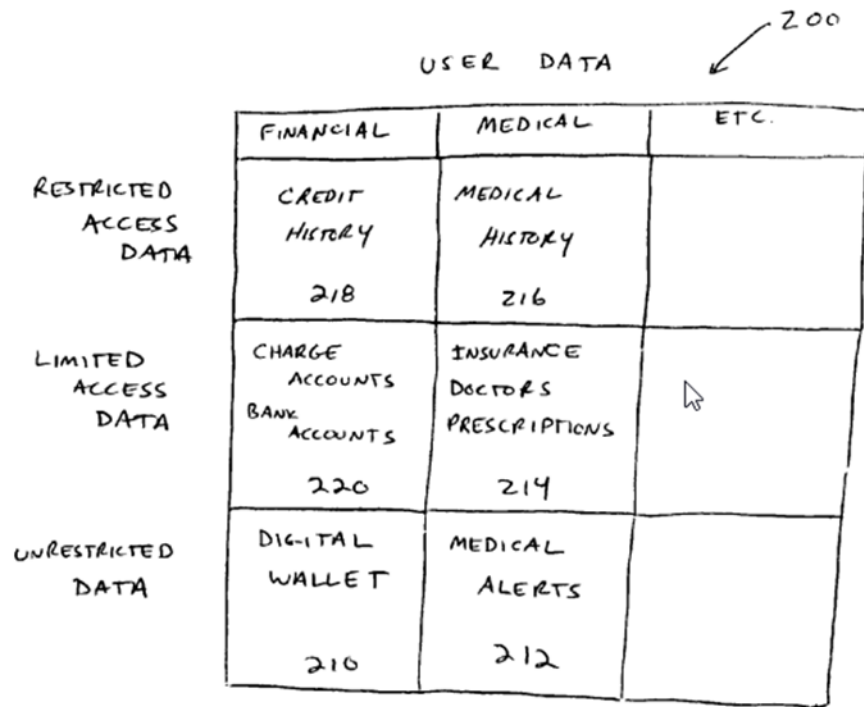


FIG. 3

Figure 3 shows a schematic diagram of partitioned server database 10 in Figure 1. *Id.* at 4:43–44. Each smart card 12 used with the system provides data pointers to the relevant partitions of central database server 10. *Id.* at 2:58–60. In operation, once the user's authorization has been verified, data pointers on smart card 12 provide access to the relevant partitioned memory portions of central database server 10. *Id.* at 3:63–66. Data from these various locations is supplied back to smart card terminal 14, and if appropriate, the data stored on the smart card 12 is updated. *Id.* at 4:3–6.

3. Asserted Obviousness of Claims 1, 5, 25, 26, 30, 50 Over Merenda (Ground 1)

In its Ground 1, Petitioner provides an element-by-element analysis of Merenda in relation to the challenged claims. Pet. 14–36. Petitioner contends, *inter alia*, “Merenda discloses extracting, e.g., parsing, security

sensitive content, e.g., private elements, from user data to obtain subsets of extracted data.” *Id.* at 27 (emphases and color highlighting omitted).

According to Petitioner, “Merenda discloses that private data (e.g., extracted data) has a plurality of security levels, and the system extracts private data for each corresponding security level.” *Id.* at 29 (emphases and color highlighting omitted). Petitioner then contends that “Merenda discloses permitting full or partial reconstruction of data by combining the public and part or all of the private data, when the requester has associated security clearance.” *Id.* at 32 (emphases and color highlighting omitted). Petitioner contends that “[a] POSITA would have understood that to reconstruct (e.g., assemble) data, which includes private data sets, Merenda’s method would access the respective extract stores for the corresponding security levels . . . , which would suggest using the associated security clearance to access the corresponding extract store.” *Id.* at 33(emphases and color highlighting omitted).

Patent Owner contends that, in Merenda, “[b]ecause the pieces information entered in the different fields on the web form are never stored as a coherent whole, and instead immediately route to a data set, there is no extraction.” Prelim. Resp. 40. Patent Owner then contends that “because there is no extraction from a whole data set having security sensitive content, there can be no ‘reconstruction.’” *Id.* at 44 (citing Ex. 2004 ¶ 75).

We focus on the “extracting” and “reconstruction” limitations in independent claim 1, and similarly recited in independent claim 26.

a) Extracting Limitation

Claim 1 recites, *inter alia*, “extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder

data.” Ex. 1001, 24:33–35. Claim 26 recite a similar limitation. *Id.* at 26:20–22.

We do not find compelling Petitioner’s contention that “Merenda discloses and/or renders obvious” the extracting limitation. Pet. 27–30. In particular, we do not find compelling Petitioner’s contention that “Merenda discloses extracting, e.g., parsing, security sensitive content, e.g., private elements, from user data to obtain subsets of extracted data, e.g., address, credit card or social security number and remainder data, e.g., non-private elements.” *Id.* at 27 (citing Ex. 1006 ¶ 23 (“[a] set of data may be parsed into private and non-private elements.”) (emphases and color highlighting omitted)).

We do not agree with Petitioner that Merenda discloses data parsing, wherein “data may be parsed into private and non-private elements.” Pet. 27; *see* Ex. 1006 ¶ 23. In particular, Merenda discloses two kinds of data parsing, one “simplistic” and the other “sophisticated”:

Fundamental to the implementation of the present invention is the notion that a set of data may be parsed into private and non-private elements. At the most simplistic level this might entail, for example, identifying input fields on a Web page as requiring sensitive data input such as an address, credit card or social security number, versus non-sensitive information such as the name of the item being purchased, the date, time etc. At a more sophisticated level this notion might entail the combination of otherwise non-sensitive data elements into a combined sensitive data construct.

Ex. 1006 ¶ 23. That is, Merenda’s “simplistic” data parsing entails identifying input fields on a Web page as requiring sensitive data input, while “sophisticated” parsing entails the combining non-sensitive data elements. *Id.* Thus, we agree with Patent Owner that Merenda’s

“sophisticated version of ‘parsing’” does not extract, as required by the claims 1 and 26, because it “doesn’t remove anything, it *combines* data fields.” Prelim. Resp. 42 (citing Ex. 2004 ¶ 70); *see* Ex. 1006 ¶ 23.

We agree further with Patent Owner that Merenda’s “simplistic” version of “parsing” also does not disclose the extracting limitation of claims 1 and 26. Prelim. Resp. 41-44. In particular, Merenda discloses storing data entered in empty fields pre-designated as “private” separately from data entered in fields pre-designated “public.” Ex. 1006 ¶¶ 23, 24, 26, 31, Figs. 1–3. As Dr. Easttom testifies, no extracting takes place because the customer has already separated the private data from the public data in filling out the web form and entering data in separate fields that were previously designated either private or public. *See* Ex. 2004 ¶¶ 58–64 (discussing Merenda). We agree with Dr. Easttom’s analogy to an airport security process:

Merenda works a bit like standard versus pre-check security at the airport. Before the security lines form, the official is trained to recognize that boarding passes with the green “pre-check” icon may enter the pre-check security line, and that those with boarding passes missing that icon should go to the regular security line. This step is analogous to what Merenda describes as its “parsed” step, meaning parsing in advance what kinds of information/boarding passes will qualify for different treatment. As people (like individual items of information) arrive, depending on what’s on their boarding pass, they go directly to either the pre-check security line (like the private data set) or the standard security line (like the public data set).

Id. ¶ 64. Petitioner presents no compelling argument that Merenda’s disclosure of storing data entered in fields pre-designated as “private” separately from data entered in fields pre-designated “public” discloses or suggests the extracting limitation.

For the foregoing reasons, we conclude that Petitioner has not provided compelling evidence to support its contention that Merenda teaches “extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data” recited in claims 1 and 26.

b) Reconstruction Limitation

Claim 1 also recites “permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores.” Ex. 1001, 24:40–44. Claims 26 recites the same limitation. *Id.* at 26:27–3.

Petitioner contends that “Merenda discloses providing partial access to data and/or providing full access to the data.” Pet. 34. Petitioner continues, “Merenda also discloses permitting reconstruction of the data into an output Web page provided to a user,” wherein a person of ordinary skill would have understood that “the output Web page would be present at the merchant computer,” and that “the consumer entering the data on their personal computer would have also been able to access the data (e.g., *reconstruct the data*) on their *personal computer* after entering it.” *Id.* at 34–35 (citing Ex. 1003 ¶¶ 193–202).

We find the reference in Merenda to providing access to data is not a compelling disclosure of reconstruction of data. In particular, we agree with Patent Owner’s contention that in Merenda, “[t]he act of viewing information in these databases does not reconstruct the original web form in whole or in part.” Prelim. Resp. 47 (citing Ex. 2004 ¶ 76). As Dr. Easttom testifies, in Merenda’s first embodiment, “[g]etting access for viewing items of information is not ‘reconstruction.’” Ex. 2004 ¶ 76. As Dr. Easttom explains, Merenda “describes merely providing access to single items of information, one at a time, not anything that is even analogous to

reconstruction.” *Id.* ¶ 77 (quoting Ex. 1006 ¶ 29, stating that “[a]ccess to the data elements . . . may be made on an element-by-element basis”).

In Merenda’s alternative embodiment, the merchant receives an email with a URL to a web page with key-coded information from the public and private data sets the merchant is authorized to see. Prelim. Resp. 47 (citing Ex. 1006 ¶ 30). We do not find compelling Dr. Zadok’s testimony that “Merenda discloses permitting reconstruction of the data into an output Web page provided to a user.” Ex. 1003 ¶ 197 (citing Ex. 1006 ¶ 10). We agree with Patent Owner and Dr. Easttom that the language of the challenged claims requires reconstruction of data objects as they existed prior to the extraction step. Prelim. Resp. 44; Ex. 2004 ¶ 82. For example, claim 1 requires “permitting full or partial reconstruction of said data.” *See* Ex. 1001, 24:40. We agree with Patent Owner’s argument that the antecedent for “said data” in the reconstruction limitation is the same “data having security sensitive content” processed in the extracting step. Prelim. Resp. 44; Ex. 2004 ¶ 75.

As Dr. Easttom explains, even accepting Petitioner’s view that the user’s filled-out Web form constitutes the original “data,” there is no reconstruction of “said data,” i.e., the web form initially submitted by the customer. Ex. 2004 ¶¶ 81–84. He testifies that “Merenda’s . . . description of that ‘customized Web page’ with public and private data aggregated for the merchant is different from the customer’s original data-entry web form.” *Id.* ¶ 85. We agree with Dr. Easttom that “[i]t is an entirely new construct, with an entirely different data structure.” *Id.* As Dr. Easttom explains, “while some of the items of information may have been the same as those provided on the original customer web form, the entire data structure is

different. This customized Web page is something entirely new, not a reconstruction.” *Id.*

For the foregoing reasons, we conclude that Petitioner has not provided compelling evidence to support its contention that Merenda teaches “permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores” as recited in claims 1 and 26.

4. Asserted Obviousness of Claims 1, 5, 25, 26, 30, 50
Over Bossemeyer (Ground 2) or Bossemeyer in view of
Merenda (Ground 3)

In its grounds 2 and 3, Petitioner provides an element-by-element analysis of Bossemeyer “alone or in combination with Merenda” in relation to the challenged claims. Pet. 36–77. In particular, Petitioner contends “Bossemeyer discloses partitioning or separating (*e.g.* extracting), data.” *Id.* at 55 (emphases and color highlighting omitted). Petitioner contends that “[person of ordinary skill] would have understood that Bossemeyer’s method parses received information into private and non-private elements.” *Id.* at 59. Petitioner then contends that “Bossemeyer discloses permitting the reconstruction of the partitioned data, *e.g.*, allowing access to the partitioned data.” *Id.* at 63 (emphases and color highlighting omitted). Specifically, Petitioner contends that “Bossemeyer discloses that partitioned data is retrieved from the extract stores of the central database server 10, and is presented, *e.g.*, at a terminal, based on a particular user’s authorization.” *Id.* (emphases and color highlighting omitted).

Patent Owner contends “Petitioner’s argument for extraction is based on it misconstruing Bossemeyer’s use of the word ‘partition,’ equating it first to ‘separating’ and then to ‘extracting.’” Prelim. Resp. 28. According

to Patent Owner, “a ‘partition’ is just a logical separation of different areas of *memory*.” *Id.* at 29 (citing Ex. 2004 ¶ 30). Patent Owner then contends that “[t]o establish ‘reconstruction of some or all said data,’ . . . Petitioner would need to prove that its hypothetical merged data is in the same form as what originally existed before any extraction step and before storage in the partitioned memory.” *Id.* at 38. According to Patent Owner, “because . . . Bossemeyer lacks ‘extraction,’ it cannot have ‘reconstruction.’” *Id.* (citing Ex. 2004 ¶ 43).

Similar to our analysis for ground 1, for grounds 2 and 3, we focus on the “extracting” and “reconstruction” limitations in claims 1 and 26.

a) Extracting Limitation

Petitioner contends that “Bossemeyer discloses partitioning or separating (e.g., extracting), data in terms of the data’s level of security/accessibility.” Pet. 55–56 (citing Ex. 1005, 2:17–27; Ex. 1003 ¶¶ 266, 267, 277, 287, 350) (emphases and color highlighting omitted). According to Petitioner, the “limited access” information and/or “proprietary information” in Bossemeyer’s database corresponds to the recited “extracted data,” and the “public” information corresponds to the recited “remainder data.” *Id.* at 56–58 (color-coded versions of Bossemeyer’s Figures 1 and 3). Petitioner asserts that “a POSITA would have understood that Bossemeyer’s method parses received information into private and non-private elements.” *Id.* at 59 (citing Ex. 1006 ¶ 7; Ex. 1003 ¶¶ 274–275).

We do not see compelling evidence from Petitioner that the extracting limitation is taught or suggested by Bossemeyer. As discussed *supra*, in Section I.C, the ’482 patent discloses extraction occurring as an initial step in which a filter removes or extracts security-sensitive data from a data object prior to storage. *See* Ex. 1001, 14:41–47, Fig. 1A. In contrast, as Dr.

Easttom, points out, Bossemeyer discloses a “partitioned” memory (*see* Fig. 3, reproduced *supra*, in Section III.C.2), but does not disclose extracting, i.e., filtering or separating, security sensitive information from source data to obtain extracted data and remainder data. *See* Ex. 2004 ¶ 29 (“Bossemeyer is entirely silent as to where the information stored in the central server comes from, the form it takes before it gets to the central database server, or how the different pieces of information end up in the different partitioned areas of memory.”). Petitioner points to no disclosure or suggestion that the “limited access” and/or “proprietary” information in Bossemeyer’s database has been filtered or separated from the “public” information, so as to result in “extracted data” and “remainder data,” as recited in the challenged claims.

Petitioner’s analysis of this claim element in light of Bossemeyer repeatedly refers to Bossemeyer’s “partitioned” database server and attempts to equate “partitioning” with “extraction.” *See, e.g.*, Pet. 56. We agree with Dr. Easttom, who testifies, “a partitioned memory does not imply or suggest extraction.” Ex. 2004 ¶ 30. As Dr. Easttom explains, a partitioned memory “merely refers to memory with different areas reserved for different types of information.” *Id.*

Petitioner further argues that, to the extent Bossemeyer does not explicitly disclose “extracting data,” a person of ordinary skill would have understood that, when Bossemeyer’s central data base server “partitions” user information in terms of accessibility, “Bossemeyer method would filter and extract the secure sensitive information . . . from the received user data.” Pet 59 (citing Ex. 1005, 2:17–20; Ex. 1003 ¶¶ 274–275). We find the reference in Bossemeyer to “partitions” is not a compelling disclosure of extracting. We agree, instead, with Dr. Easttom, that this disclosure in

Bossemeyer is “merely referring to the act by the memory partitions of keeping different pieces of information separate from each other, not removing some pieces of data from a larger whole.” Ex. 2004 ¶ 32. As Dr. Easttom testifies, “POSITA would have understood that the extraction process of the ’482 Patent is vastly different than the act of ‘partitioning’ either as used in Bossemeyer or as used in the art at the time.” *Id.* ¶ 34.

For the foregoing reasons, we conclude that Petitioner has not provided compelling evidence to support its contention that Bossemeyer teaches “extracting said security sensitive content to obtain extracted data for each corresponding security level and remainder data” recited in claims 1 and 26.

b) Reconstruction Limitation

Petitioner contends that Bossemeyer discloses the “reconstruction” limitation. Pet. 63–67. In particular, Petitioner contends that “Bossemeyer . . . discloses permitting the reconstruction of the partitioned data, e.g., allowing access to the partitioned data, only in the presence of an associated security clearance, e.g., user identification/ authentication code or authorization/access code associated with a particular security level.” *Id.* at 63 (citing Ex. 1005, 2:38–47; Ex. 1003 ¶¶ 285–289) (emphases and color highlighting omitted).

We do not find this argument compelling for several reasons. First, Petitioner’s argument equates “reconstructing” with “allowing access” to the user data. Pet. 63. We do not agree. As Dr. Easttom testifies, “[p]roviding access to data, or allowing someone to view it, is not reconstruction.” Ex. 2004 ¶ 46. Dr. Easttom continues, “[n]othing in Bossemeyer suggests that the piece of data targeted by the pointer and then provided to the

merchant is in any way reconstructed or combined with any other data, let alone a body of data that it was originally a part of.” *Id.*

We are also not persuaded that Dr. Zadok’s testimony provides compelling evidence that this limitation is met by Bossemeyer. *See* Ex. 1003 ¶¶ 284–301. We agree with Patent Owner that much of Dr. Zadok’s testimony is based on assumptions that he does not support with facts. Prelim. Resp. 35–37. For example, he testifies, without factual support, that

The system of Bossemeyer retrieves remainder data (e.g., public information such as a customer’s name), retrieve [sic] extracted data (e.g., proprietary or limited access information such as credit card numbers and account PIN/numbers), and then logically merges these pieces of information (i.e., reconstruct the original information to appear as before it was split into different security categories).

Ex. 1003 ¶ 297 (emphases and color coding omitted). Dr. Zadok provides no citation to Bossemeyer, and we see no disclosure that Bossemeyer’s system “logically merges” public information, such as a customer’s name, with proprietary or limited access information, such as credit card numbers and account PIN/numbers. *Id.* Dr. Zadok even admits that “Bossemeyer does not explicitly state that the information, once reaching the terminal, is merged/reconstructed.” *Id.* ¶ 298. Nevertheless, he speculates (without support) that “a POSITA would have understood that such logical merging would have been obvious to take place for the (secure) transaction to succeed.” *Id.*

Similarly, we are not persuaded by Dr. Zadok’s testimony that “Bossemeyer discloses permitting reconstruction of some of a user’s medical data (e.g., data including the user’s medical alerts 212, and insurance and

prescription information 214) and permitting reconstruction of all of user's data (e.g., data further including the user's medical history 216) with additional authorization.” Ex. 1003 ¶ 300 (emphases and color highlighting omitted). We find that Dr. Zadok's testimony is speculative, hindsight-biased, and unsupported by Bossemeyer, which does not disclose or suggest any such logical merging of data. *See, e.g., Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1354 (Fed. Cir. 2013) (holding that an articulated reasoning “is especially important to guard against the dangers of hindsight bias”); *see also* Ex 2004 ¶¶ 47–56 (challenging Dr. Zadok's assumption of merging data in Bossemeyer).

We agree with Patent Owner that Petitioner fails to address where the various pieces of information in Bossemeyer's partitioned database came from or their form before the alleged extraction and storage, making it impossible to “reconstruct” that which never existed previously. Prelim. Resp. 38–39; Ex. 2004 ¶ 53 (“Bossemeyer is entirely silent on the nature of the data before it is found in the portioned database server.”).

For the foregoing reasons, we conclude that Petitioner has not provided compelling evidence to support its contention that Bossemeyer, alone or in combination with Merenda, teaches “permitting full or partial reconstruction of said data with corresponding extracted data and remainder data after accessing said respective extract stores” recited in claims 1 and 29.⁵

⁵ In view of this determination, we do not need to address Patent Owner's additional argument that Bossemeyer is not analogous art to the '482 patent. Prelim. Resp. 16–24. Similarly, we do not need to address Patent Owner's additional argument that a person of ordinary skill would not have found it obvious to combine Merenda with Bossemeyer. Prelim. Resp. 50–61.

5. Summary

Based on the record before us, Patent Owner has raised substantial issues with Petitioner’s analysis of the challenged independent claims, so that the evidence does not plainly support Petitioner’s position. As discussed above, “[c]ompelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.” Guidance Memo, 4. For the reasons given, we determine that Petitioner has not presented a “compelling, meritorious challenge[]” to any claim of the ’482 patent. *Id.* Accordingly, we find that the sixth *Fintiv* factor does not weigh against discretionary denial.

D. Balancing the Fintiv Factors

We have considered the circumstances and facts before us in view of the *Fintiv* factors. As discussed above, we have determined that factors 1–5 weigh in favor of discretionary denial of institution. Moreover, we have further determined that the Petition does not show compelling evidence of unpatentability under factor 6. We therefore conclude that the evidence of record favors exercising our discretion to deny institution of an *inter partes* review.

IV. CONCLUSION

Upon consideration of the Petition, the Preliminary Response, and the evidence presented, we exercise our discretion under 35 U.S.C. § 314(a) to deny institution of an *inter partes* review challenging claims 1, 5, 25, 26, 30, and 50 of the '482 patent.

V. ORDER

For the foregoing reasons, it is hereby:

ORDERED that the Petition is *denied*, and no trial is instituted.

IPR2023-00970
Patent 7,552,482 B2

FOR PETITIONER:

Theodoros Konstantakopoulos
Brian Matty
DESMARAIS LLP
tkonstantakopoulos@desmaraisllp.com
bmatty@desmaraisllp.com

FOR PATENT OWNER:

Ragnar Olson
GLOBAL IP LAW GROUP, LLC
rolson@giplg.com