UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

INTERNATIONAL BUSINESS MACHINES CORPORATION
Petitioner
v.
DIGITAL DOORS, INC.
Patent Owner

_____

IPR2023-00969
U.S. Patent No. 7,349,987
PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

EXPERT DECLARATION OF DR. WILLIAM C. EASTTOM II (CHUCK EASTTOM) PH.D., D.SC.

IBM v. Digital Doors
IPR2023-00969, 7,349,987
DigitalDoors EX2004

II. INTRODUCTION

1. I have been retained by counsel for DigitalDoors, Inc. ("DigitalDoors" or "Patent Owner") and asked to provide my opinion on the validity of claims 1, 6, 9, 10-11, 15-16, 21-23, and 27 of U.S. Patent No. 7,349,987 in view of four references, U.S. Patent No. 7,010,701 ("Bossemeyer," EX1005), U.S. Publication No. 2004/0148290 ("Merenda," EX1006), U.S. Patent No. 6,845,488 ("Chaganti," EX1007), and U.S. Publication No. 2004/0199765 ("Kohane," EX1008).

2. To conduct my analysis, I reviewed the '987 Patent, Bossemeyer, Merenda, Chaganti, and Kohane. I also reviewed the Petition for *Inter Partes* Review and the accompanying Declaration of Dr. Erez Zadok (EX1003). A full list of the materials that I reviewed is attached as Appendix A.

III. BACKGROUND AND QUALIFICATIONS

3. My name is William C. Easttom II (Chuck Easttom). I have 30 years of experience in the computer science industry including extensive experience in cybersecurity. I have authored 41 computer science books, including textbooks used at over 60 universities around the world.

4. I hold a Doctor of Science degree in Cyber Security from Capitol Technology University (Dissertation topic "A Comparative Study of Lattice Based Algorithms for Post Quantum Computing"). I also hold a Doctor of Philosophy (Ph.D.) in Technology (Dissertation topic "The Effects of Complexity on Carbon

IBM v. Digital Doors
IPR2023-00969, 7,349,987
DigitalDoors EX2004

Nanotube Failures") from Capitol Technology University, and a Doctor of Philosophy (Ph.D.) in computer science from the University of Portsmouth (Dissertation topic "A Systematic Framework for Network Forensics Using Graph Theory). I also hold three master's degrees (one in Applied Computer Science, one in Education, and one in Systems Engineering). I am an inventor with 25 computer science patents.

5. I also hold over 70 industry certifications, including several related to computer security. I am also experienced in database management and data mining.

6. I am a Distinguished Speaker for the Association of Computing Machinery (ACM) and a Senior Member of the Institute for Electrical and Electronics Engineering (IEEE) and a Senior Member of the Association of Computing Machinery (ACM). The IEEE is the world's largest and most preeminent engineering organization. Among other activities, the IEEE creates industry standards including hardware, software, and other engineering and computer science standards. I am also a Distinguished Visitor of the IEEE. I have been a member of the IEEE Software & Systems Engineering Standards Committee for several years. I worked on the DevOps 2675 standards group from 2017 to 2019. I am also currently the Vice Chair of the IEEE p23026 Standards Group "Systems and Software Engineering -- Engineering and Management of Websites for Systems, Software, and Services Information." I am also a Member of the IEEE Engineering

in Medicine and Biology Standards Committee, Standard for a Unified Terminology for Brain-Computer Interfaces P2731, from 2020 to present. I chair one of the subgroups.

7. I am an adjunct lecturer at Georgetown University, teaching graduate courses in *Requirements Engineering* and *Cryptography*. I am also an adjunct professor at Vanderbilt University teaching graduate computer science courses, including a course in *quantum computing* and a graduate course in *digital forensics*.

8. During the time period of 1996 to 2000, I worked for Boeing Aerospace on software for the NATO AWACS program, Alegis Systems Group as a Sr. Software Engineer, and as Director of Academic computing for Southeastern Oklahoma State University. While working at NATO AWACS, data security was a key concern. When I was working at Alegis Systems Group, I was developing software for banks. This provided me with an understanding of financial software and transactions. Due to personally identifiable information, financial information, and other sensitive information being processed, security was a substantial concern. While working as Director of Academic computing for SOSU, I was responsible for all cybersecurity for the university including authentication and authorization methods.

9. From 2007 to 2009 I worked extensively with medical software including Electronic Medical Records (EMR) and medical billing. Furthermore, my

second master's degree included a semester research project in electronic medical software.

10. In addition to the summary, I have provided here, I describe my qualifications, issued patents, publications, and experience as an expert witness in greater detail in my curriculum vitae ("CV") attached as Exhibit 2005.

IV. MATERIAL CONSIDERED

11. In forming my opinions, I have considered the following:

- U.S. Patent 7,349,987, EX1001
- The petition for IPR2023-00969
- All exhibits to that petition.
- The expert declaration of Dr. Erez Zadok, EX1003
- All exhibits to that declaration
- Any references cited in this declaration.

V. SUMMARY OF OPINIONS

12. All claims of the '987 Patent require an "extracting/parsing" step and a "reconstruction" step. Neither step, however, is present in the Bossemeyer reference and the "reconstruction" step is not present in the Merenda reference, as detailed below.

13. Both the Bossemeyer and Merenda references are from fields dramatically divergent, both from the technology of the challenged patent, as well

as from each other. Bossemeyer is in the field of smart card applications. EX1005, 1:6-10. Merenda concerns Internet eCommerce and targeted email marketing. EX1006, ¶4. The '987 Patent concerns data security for systems with large amounts of data, like email systems, browser programs, and telecommunications programs. EX1001, 1:14-22, 9:34-35. Persons of skill in the art of the '987 Patent would not have looked to either of these references for combinations, nor would one working with Bossemeyer have looked to Merenda's field of art for combinations with Bossemeyer, as the petition and Dr. Zadok contend. Moreover, because these two references come from such different fields, combining them would not have made sense for a variety of practical reasons.

VI. REFERENCES AT ISSUE

14. As noted above, the field of the '987 Patent concerns data security for systems with large amounts of data, like email systems, browser programs, and telecommunications programs. EX1001, 1:14-22. More specifically, it concerns the processing, distribution, and secure storage of files/documents/data objects across telecommunications networks. EX1001, 1:14-22. Its prime focus is "securing data in a computer system." EX1001, 7:42. The '987 Patent specification describes securing data on a single computer, or a plurality of computers linked over a LAN or WAN in a manner that is flexible and programmable by the user. EX1001, 6:34-38, 45-57. For these reasons, the lead PTO's lead Class for it is 709, "Electrical

Computers and Digital Processing Systems: Multicomputer Data Transferring." Within that class, the USPTO subclass is 244 for "Centralized Controlling" for such information security systems. The USPTO describes that subclass as "subject matter wherein one computer selects the path used for data transfer by each of the other computers."[1] The challenged '987 Patent claims are all either method claims or computer readable medium claims for practicing a method. The challenged claims generally accomplish that method in part by "extracting security sensitive data" from the original data and later reconstructing the original "data" in the presence of appropriate security clearance.

15. The petition's primary/lead reference is Bossemeyer. Bossemeyer describes its technical field as "Smart card applications and, more particularly, to a network arrangement to provide access to an architecture that Supports a variety of advanced Smart card applications." EX1005, 1:7-11. "Smart cards" are "substitute, replacement, or consolidation cards" for credit/debit/ATM cards as well as car rental, hotel, and airline membership cards. EX1005, 1:17-20, 27-31. They hold "much more information" than conventional magnetic stripe cards and "often include some 'intelligence' such as a microprocessor." EX1005, 1:34-38. The

[1]https://web.archive.org/web/20080208014715/http://www.uspto.gov/web/patents/classification/uspc709/defs709.htm, EX2009.

USPTO's lead Class for Bossemeyer is 713, "Electrical Computers and Digital Processing Systems: Support." Its subclass within that Class of support for electrical computers and digital processing systems is 201, "for computer network security in general or in combination with nominal cryptography."[2] Bossemeyer teaches a network connecting a smart card reader terminal through a phone network or the internet to a central storage server. EX1005, Figs. 1, 2.

16. The petition's secondary reference is Merenda, which the petition points to for elements to the extent they are not present in Bossemeyer. Merenda is a division of an application titled "Sending Advertisements to Customers Identified by a Non-Viewable Database." EX1006, ¶1. It seeks to provide a solution to a problem still with us today: "As the Internet evolves into the dominant commercial medium, merchants seeking to leverage data about Internet user's [sic] to better focus their marketing efforts must do so in a manner that respects the privacy interests of their intended customer." EX1006, ¶4. Merenda's USPTO primary Class is 707, "Data Processing: Database and File Management or Data Structures."

[2]https://web.archive.org/web/20050422055224/http://www.uspto.gov/web/patents/classification/uspc713/defs713.htm, EX2010.

Its subclass is 10, "distributed or remote access."[3] Its solution is a "program product for 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" or to simply "read entries in the private data set." EX1006, ¶2

17. A POSITA would immediately note that the '987 Patent, Bossemeyer, and Merenda are all three in separate fields with no overlap. This is clear in the patents' own descriptions as well as in the USPTO classifications. As I discuss in more detail below, a POSITA working in the '987 Patent's field would not have looked to the fields of Bossemeyer. Nor would someone working in the field of Bossemeyer have looked to the field of Merenda for solutions. It is also most probable that a POSITA in the '987 Patent's field would not have been a POSITA in the field of Bossemeyer/Carmichael. This is described in more detail later in this declaration.

VII. POSITA

18. The petitioner has asserted that "A Person of Ordinary Skill In The Art ("POSITA") would have had a bachelor's degree in computer science, computer engineering, electrical engineering, or equivalent, and approximately two years of

[3]https://web.archive.org/web/20041108063552/http://www.uspto.gov/web/patents/classification/uspc707/defs707.htm, EX2011.

experience working in the field of data storage systems and data security as of November 13, 2000. Less professional experience can be substituted by additional education, and vice versa." Pet., 8.

19. For the purposes of this declaration, I will use that definition of a POSITA without conceding that it is necessarily correct.

VIII. ANALYSIS

A. Extraction and Reconstruction in the Challenged Claims

20. I understand that the Petitioner has challenged the validity of Claims 1, 6, 9, 10, 11, 15, 16, 21, 22, 23, and 27 of the '987 Patent. Claims 1, 10, 16, and 22 are independent claims. I present Claim 1 below as an example of the steps these claims generally cover:

> 1. A method of securing data having one or more security sensitive words, characters or icons in a computer system with a plurality of physically distinguishable memories respectively designated as a remainder store and a plurality of physically distinct extract stores corresponding to a plurality of security levels for respective subsets of said security sensitive words, characters or icons comprising:
>
> extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;
>
> storing said extracted data and said remainder data in said respective extract stores corresponding to an associated security level and said remainder store, respectively; and,

permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data only in the presence of a predetermined security clearance corresponding to said associated security level for said respective extract stores.

21. Like Claim 1 above, the other independent claims include an "extracting/parsing" step with similar claim language:

Claim 1	extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;
Claim 10	parsing said data to obtain extracted data for respective associated security levels and remainder data therefrom;
Claim 16	extracting said security sensitive words, characters or icons from said data to obtain extracted data and remainder data therefrom;
Claim 22	parsing said data to obtain extracted data for respective associated security levels and remainder data therefrom;

22. Also, like Claim 1 above, each independent claim also includes a "reconstruction" step with identical claim language:

Claim 1	permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data…
Claim 10	permitting full or partial reconstruction of said data via said extracted data from said respective extract stores and remainder data…
Claim 16	permitting full or partial reconstruction of said data via said extracted data from respective extract stores and remainder data…

Claim 22	permitting full or partial reconstruction of said data via said extracted data from said respective extract stores and remainder data…

23. At least these two critical elements are absent from Bossemeyer and the reconstruction element is absent from Merenda.

B. Absence of Extracting/Parsing and Reconstruction in Bossemeyer

24. As explained briefly above, Bossemeyer concerns "smart card applications using a smart card in combination with a smart card terminal." EX1005, Abstract. One example of the state of smart-card technology at the time of Bossemeyer is an academic paper written by Major McClannan, in which he discusses his perspective that the U.S. Airforce Reserve should consider implementing smart cards.[4] What is noteworthy is that in 2001 this was still technology that even the U.S. Air Force reserve had not implemented. Knowledge of this technology was quite specific and was not widely known or used at the time.

25. In Bossemeyer's smart-card setup, a smart card reader/terminal would connect through a network central office of a standard public-switched telephone network to a central database server accessible to different merchants, as shown in Bossemeyer's Figure 1:

[4] "Implementing Smart Cards Into the Air Force Reserve" at https://apps.dtic.mil/sti/pdfs/ADA406328.pdf, EX2012

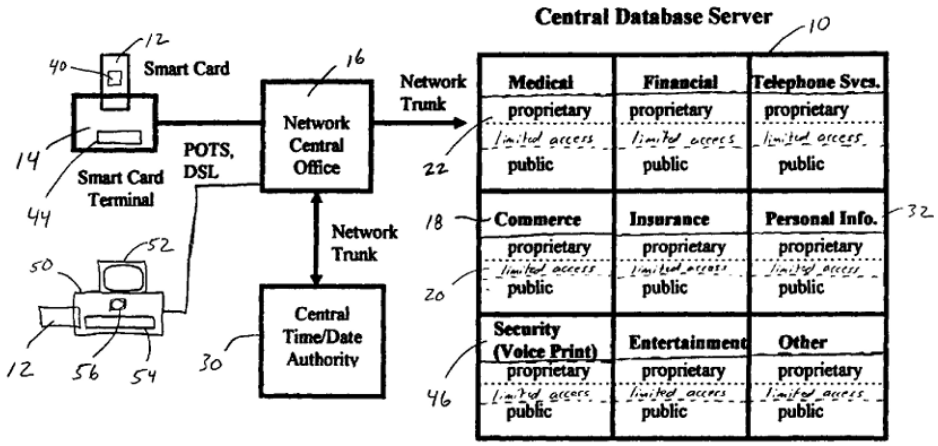


Figure 1

See also EX1005, 2:4-12.

26. That central database server's memory was partitioned, with different types of information stored separately in different areas of the memory. EX1005, Fig. 1, 2:13-36. Some of the information, such as personal medical information, would be considered private or proprietary. EX1005, 2:27-36. Bossemeyer's Figure 3 shows varied levels of privacy related to different types of data:

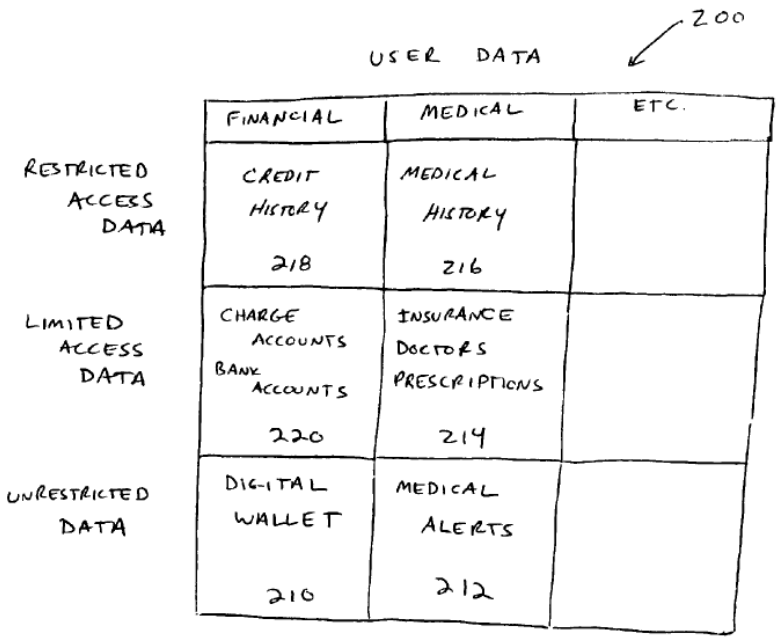


FIG. 3

27. Bossemeyer's setup worked like this. A user's smart card stored pointers to different areas of the central server's memory. EX1005, 2:58-60. When a user put the card in the merchant's reader device, the reader would read those pointers. If the card had pointers to the private/proprietary portions of the server memory, that data from that portion of the memory would then be sent back to the location of the merchant's smart-card reader/terminal. EX1005, 4:3-6. Effectively, the pointers on the smart card provided the key to access that private data. EX1005, 3:18, 63-66. A customer in a store would pick up an item to purchase, go to checkout, and present his or her smart card. The smart card terminal or reader reads information stored on the smart card. EX1005, 3:39-41. The smart card terminal then communicates with a remote server to obtain information to complete the

IBM v. Digital Doors
IPR2023-00969, 7,349,987
DigitalDoors EX2004

transaction, and the customer can then leave with the item. EX1005, 3:43-51. Other examples of the type of transactions that Bossemeyer's smart card system facilitates are payments at gas stations, grocery stores, department stores, and hotels. EX1005, 1:19-21, 5:16. For in-person transactions like these, speed and ease of the transaction are important.

28. The petition and Dr. Zadok point to two different parts of Bossemeyer to argue that it teaches extracting/parsing of some data from a larger whole. First is the discussion at column 2, lines 17-33 and 40-47 of Bossemeyer, which discuss the partitioned memory and what kind of information the central database stores. Second are Figures 1 and 3, which further discuss that notion of partitioned memory and merely illustrate the kinds of information stored in the central database server.

29. The problem is that neither of these Bossemeyer citations relates to extracting some data from a larger whole. The '987 Patent's claim element in question here is the method-type step of extracting some data from an original "data." Yet 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. The petition and Dr. Zadok seem to assume that the pieces of information come from some pre-existing collection of "data" from which individual pieces of information are removed for storage, but Bossemeyer never talks about

such a collection or suggests that the pieces of information were removed from a larger collection before they were stored in the individual partitioned areas of memory. In other words, Bossemeyer is entirely silent about the steps that the challenged '987 Patent claims detail, what is happening to the data from processing (the extraction step) through storage. In Bossemeyer, pieces of information are already in storage.

30. The petition and Dr. Zadok try to find extraction in Bossemeyer's description of "partitioned" memory, but a partitioned memory does not imply or suggest extraction or parsing of data. A partitioned memory was and is well known in the art. It merely refers to memory with different areas reserved for different types of information. Dr. Zadok's own evidence supports this conclusion. He points to the definition of "parse" on a page from a Microsoft technical dictionary. EX. 1003, ¶157. But he doesn't mention the definition of "partition," the word he's relying on from Bossemeyer, found on that same page. EX. 1003, ¶157. It defines "partition" as a "logically distinct portion of memory or a storage device that functions as though it were a physically separate unit." EX. 1028, 24. That same dictionary that Dr. Zadok attaches also separately defines "disk partition" in a similar manner, as "[a] logical compartment on a physical disk drive. A single disk might have two or more logical disk partitions, each of which would be referenced with a different disk drive name." EX 1028, 7. That definition is consistent with multiple contemporary

sources.[5, 6] A "partition" and "partitioning" in the art, therefore, refer to the logical separation of different areas of memory.

31. Bossemeyer's Figures 1 and 3 show partitioned memory with different locations for different kinds of information. Its repeated references to "partitions" in the server memory are consistent with that understanding. (*See, for example,* EX1005, 2:40 "partitions in the database"; 2:60 "partitions of the central database server"; 3:58-60 "The desired application is then selected which relates to a memory partition of the central database server"; 3:65-66 "access to the relevant partitioned memory portions of the central database server"; 4:17-18 "pointers to relevant data within the partitioned central database server"; 4:43-44 "FIG. 3 shows a schematic diagram of the partitioned server database").

32. The petition and Dr. Zadok don't discuss any of these definitions or any of these instances of "partition" in the patent. Instead, they point to a single use of

[5] Posey, B. (2000). All about partitions: The right FAT can save your waste. Retrieved from https://www.techrepublic.com/article/all-about-partitions-the-right-fat-can-save-your-waste, EX2013.

[6] Walker, M. (2000). Splitting Your PC Data Across Multiple Drives & Partitions. Retrieved from https://www.soundonsound.com/techniques/splitting-your-pc-data-across-multiple-drives-partitions, EX2014.

the term in a verb form, "partitioning," "a centralized partitioned database server which partitions information." EX1005, 2:17-18. They infer from that statement that partitioning means taking a large data set and extracting portions of that data set. But that isn't what "partitioning" means in this context, as is clear from the way that term was used by those in the art at the time, and from the way it is used everywhere else in Bossemeyer. "Partitioning" 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. Another technical dictionary from this time frame that defines "partition" as a verb (the earlier-cited dictionaries don't) as this one Bossemeyer snippet does is consistent, making clear that "partitioning" merely means sectioning up the memory, not extracting one piece of data from a larger whole: "Partition: Before a hard disk can be used for the first time, it must be partitioned and then formatted. Partitioning is a software function that involves dividing the storage space into usable sections, with each section assigned a letter as though it were a separate drive."[7]

33. That snippet that the petitioner and Dr. Zadok point to at Bossemeyer 2:17-18 about "partition[ing] information" cannot be understood to mean that some set of data is arriving at the central database server, which then intelligently breaks

[7] Prentice Hall's Illustrated Dictionary of Computing 3rd Edition (1998), EX2006.

that data set up and puts different pieces in different reserved areas. Bossemeyer provides no description or suggestion of such an extraction process, in contrast to the extensive discussion of that kind of process in the ’987 Patent. For example, the ’987 Patent explains that its “invention relates to a data security system and method and, more specifically, parsing (typically through a filter), extracting and dispersion of the parsed or segregated data with the controlled reconstruction of data utilizing security protocols to provide a system, method and programming instructions stored on computer readable medium for securing data.” EX1001, 1:14-18. It describes “establishing a group of security sensitive words, characters, icons, data streams or data objects, filtering the data input from a data input device and extracting the security sensitive data.” EX1001, 7:43-46. It provides a variety of other examples, like “[t]he method and the computer media containing programming instructions includes filtering data from the data input computer, extracting security sensitive words, phrases, characters, icons, or data objects and forming Subsets of extracted data and remainder data. The subsets of extracted data are stored in one or more computer memories in the network identified as extracted stores. The remainder data is also stored in the network if necessary.” EX1001, 8:32-40. Another example is the description of how “the invention operates as a credit card or financial data scrubber. The e-mail data has one or more security sensitive words, characters or icons and the method … extracts the security sensitive words, characters or icons

from said e-mail data to obtain extracted data and remainder data." EX1001, 9:36-43.

34. A POSITA would have understood that the extracting/parsing process of the '987 Patent is vastly different than the act of "partitioning," either as used in Bossemeyer or as used in the art at the time as the variety of technical dictionaries cited above demonstrate.

35. In fact, everywhere that Bossemeyer uses "partitioned" as a verb in relation to information, it makes clear that it's referring to that piece of information merely being stored in a different, partitioned area of memory, thereby kept separate from other pieces of information:

- "[A] merchant may require access to a user's credit information to determine whether to accept the user's credit for a particular dollar amount. This information ***may be partitioned*** in the limited access region 20 of commercial transaction applications 18." EX1005, 2:23-27 (emphasis added).

- "Private or proprietary information ***is partitioned*** such that the owner of the information has control over how the information is transferred and used." EX1005, 2:28-30 (emphasis added).

36. For at least these reasons, Bossemeyer's reference to partitioned memory cannot be understood to mean extracting/parsing parts of data from a larger whole as claimed in the '987 Patent.

37. The petition then separately makes several contentions about what a POSITA would understand:

- To the extent Patent Owner argues that Bossemeyer does not explicitly disclose 'extracting data,' a POSITA would have understood that when Bossemeyer's 'central[] database server partitions [user] information… in terms of… the accessibility of the information' (EX1005, 2:17-20), Bossemeyer teaches separating sensitive information from user data." Pet., 27.
- Moreover, a POSITA would have understood that Bossemeyer's disclosure of separating user data utilized a parsing algorithm, because Bossemeyer's method would filter and split the sensitive information, (e.g., restricted- and/or limited-data), from the received user data, (e.g., from a user data file), and store the restricted-and/or limited-data in the appropriate security-level store, while storing the remaining information in the user data file as unrestricted data, (e.g., public data). Pet., 28-29.
- For example, a POSITA would have understood that Bossemeyer's method parses received information into private (restricted, limited access data) and non-private (unrestricted data) elements. Pet., 29.

There are numerous problems with these contentions.

38. First, it's notable that the petition switches to the word "parse," even though Bossemeyer never uses that term. As noted above, Dr. Zadok's declaration at ¶157 cites to the Microsoft definition of "parse," a term which is absent in Bossemeyer, while ignoring the definition of "partition," which is in Bossemeyer and appears on the very same dictionary page and contradicts his argument. EX1028, 24.

39. While the petition and Dr. Zadok discuss "parsing" as if it were found in Bossemeyer, their quotation for support is to Merenda. In the midst of the discussion of Bossemeyer, at page 29, the petition uses a quote from EX1006, Merenda to argue that Bossemeyer teaches "parsing."

40. It is, therefore, unclear how the petitioner can argue that a POSITA would have understood Bossemeyer to imply extracting/parsing with the word "parse" when Bossemeyer never uses "parse" (or "extracting," for that matter).

41. I also understand that to argue that something is inherent, the petitioner must make clear that the missing element is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. "Extracting" or "parsing" is not inherent merely because there is partitioned memory. In my experience, data often is loaded to partitioned memory without a prior extraction/parsing step. For example, when one downloads a file from the Internet, that individual file (be it image, Adobe PDF, etc.) is downloaded to the

user's hard disk without any extraction/parsing process. As another example, when one is typing a Microsoft Word document and saves the document, that document is saved to the user's partitioned hard disk without any extraction/parsing process. Indeed, Dr. Zadok's reference to the definition of a "disk partition" (discussed above, ¶30) illustrates that such partitioning needs to occur before the disk can be used for storage. But if the petitioner's inherency argument were right, that would mean that every time one stored data on a disk, it would first need to undergo an "extraction" process (because the memories of all disks are partitioned before use). That obviously is not the case.

42. The Petition concludes this section on page 27 discussing a fictitious "user's medical data file," suggesting that such a file would have multiple pieces of information that would need to be extracted. But Bossemeyer never describes a file like this or refers to any kind of file with multiple pieces of information, and I don't find any evidence of either in the petition or Dr. Zadok's report. And when they present a modified version of Bossemeyer's Figure 3 on page 28 of the Petition and ¶158 of Dr. Zadok's declaration, it still doesn't suggest "extracting/parsing" of some pieces of information from a larger file or set of data. Even this modified figure, and the specification text they quote, merely states that these different pieces of information are stored in separate partitioned areas of the memory. But none of this

evidence from Bossemeyer suggests that, prior to being stored in the partitioned areas of memory, these different pieces of information were part of a large "file."

43. I turn now to reconstruction, a separate claim element that is absent from Bossemeyer. I first note that without an extracting/parsing step, by definition in the context of the claim, there can be no reconstruction step. If something is never pulled apart, it cannot be reconstructed.

44. Pages 43-47 of the petition and ¶¶197-209 of Dr. Zadok's declaration seek to find reconstruction in Bossemeyer. Both point exclusively to the same five quotes from Bossemeyer and Bossemeyer's Figure 3. But none of those sources suggests, implies, or teaches reconstruction.

45. The five quotes they use all essentially say the same thing. When the smart card, with its stored data pointers, is inserted in the reader, those data pointers then point to the requested information in the central database server. That server then makes that information available by allowing access/sending it back to the smart card terminal. That is all these quotes state (emphasis shown comes from the petition and Zadok's declaration):

> The structure of the central database server is similar to a UNIX-based file system. ***Different user identification codes***, or data pointers, provided by smart cards 12 ***allow access to partitions in the database***. The information contained within the central database server… can be classified as public information available to all the world; limited

access information available to persons or selected groups with a user authentication code; or proprietary information accessible only by the owner of the information or a group with privileges to that directory information. EX1005, 2:38-47.

Although the central database server 10 is shown as a single server, it is to be understood that multiple servers may comprise the central database server 10. For example, in the merchant transaction discussed above, the purchaser's credit files are more likely to be stored in a database monitored by the credit reporting companies such as TransUnion or Equifax, as opposed to the central database server 10. In such cases, ***the central database server 10 acts as a network smart card server which facilitates data transfer between the database containing the desired information and the merchant or person requesting the information.*** In the same way, insurance information would ultimately reside with the insurer, medical records with the health provider, financial records with the bank or broker, and so on. The network smart card server acts as a secured gatekeeper to such information and the smart card acts as the enabling key. EX1005, 3:3-18.

Once the user's authorization has been verified, data pointers on the smart card 12 provide access to the relevant partitioned memory portions of the central database server 10. Routing circuitry controlled by the microprocessor within the central database server 10 routes the data pointer to appropriate memory locations or database of the information keeper relating to the application at issue such as medical, financial, etc. ***Data from these various locations is supplied back to***

the smart card terminal 14, and if appropriate, the data stored on the smart card 12 is updated. EX1005, 3:63-4:6.

The network server 10, 110 validates the user identification by decrypting the authorization code. This information is then cross-referenced with the merchant code to identify the information available to the merchant. ***The merchant can then view the information stored within the server 10, 110***, upload/download information, and perform transactions which are recorded at the server 10, 110. EX1005, 4:59-65.

FIG. 3 provides one example of the type of information accessible within or through the server 200. As mentioned above, information is stored in three levels of security: unrestricted, limited access, and restricted. In the pharmacy example, once the user's authentication code and merchant code have been verified by the system, the pharmacist may have access to the user's digital wallet 210, ***medical alerts 212***, and ***insurance and prescription information*** 214. Without further authorization, however, the pharmacy would not have access to the user's ***medical history 216***. EX1005, 5:6-15.

46. It appears that the petitioner is asserting that any retrieval of a subset of data is 'reconstruction,' and that is inaccurate. Providing access to data, or allowing someone to view it, is not reconstruction. Nothing 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.

47. Dr. Zadok's declaration actually concedes that Bossemeyer does not explicitly disclose reconstruction: "Although Bossemeyer does not explicitly state that the information, once reaching the terminal, is merged/reconstructed…" EX1003 ¶205. Instead, he contends that when multiple pieces of information get returned, "logical merging would have been obvious to take place for the (secure) transaction to succeed: otherwise, why retrieve disparate information from different stores, send it to a single terminal location, only to not use it in unison, thus resulting in a failed transaction." EX1003 ¶205.

48. Dr. Zadok makes several unstated assumptions in his statement, and it is not clear that any of them are true, nor does Dr. Zadok cite any source, reference, or basis for these assumptions. First, he contends that merging would be necessary "for the (secure) transaction to succeed." EX1003, ¶205. Dr. Zadok provides no explanation and cites no evidence as to why that would be the case. Dr. Zadok points to financial transactions. However, whether or not merging would occur is dependent on the specifics of the electronic financial transactions. I do not see anything in Dr. Zadok's CV that qualifies him as an expert in financial transactions. Nowhere does his CV mention financial, banking, or any related experience, education, or training. EX1004. Conversely, in the late 1990s I worked as a senior software engineer developing financial applications for banks. It is quite clear to me that it is equally possible that each piece of data could be returned and used

separately for a separate part of the transaction process without them ever being merged. There are numerous examples specifically from financial transactions. For example, if a user is withdrawing money at an ATM, all information would come from a single source (customers bank account record) with only a single piece of information needed to allow the transaction (balance available). As another example, for a merchant charging a credit card for a purchase, the only information the merchant would need to retrieve is whether or not the balance is equal to or greater than the available funds/credit.

49. In fact, there are reasons not to merge the data. For example, Bossemeyer explicitly discusses financial data in figure 3 including restricted data such as credit history (218) and charge accounts (220). For a merchant processing a payment transaction, the only relevant issue is whether or not the charge account has a sufficient amount open to process the charge. Since this is an existing charge account, the customers credit history is not relevant to this transaction. In the case of figure 3 in Bossemeyer, merging is strongly contraindicated. Merging bank accounts, credit history, and a digital wallet put data that Bossemeyer identifies as *restricted*, *limited*, or *unrestricted*, into the same dataset. Neither Dr. Zadok nor the petition articulate any benefit or rational for doing this. Including unnecessary "restricted access" data like credit history is problematic for security reasons. It

unnecessarily leaves that data susceptible to exposure, complicates the transaction, and combines data that Bossemeyer endeavors to keep separate.

50. Furthermore, with the data described in figure 3 of Bossemeyer, the data would be difficult if not impossible to merge. Consider the Bank Account data 220 and the Digital Wallet 210. For Bank Accounts (220 in figure 3 of Bossemeyer) banks will often use BAI2 files in transmitting information.[8, 9] This file type has a specific format.[10] Banks may also use file types such as Swift MT,[11] ISO 20022,[12] NACHA[13] (National Automated Clearinghouse Association), or others. Each of these is not compatible with the others, and substantial file translation is required. The digital wallet (210 in figure 3 of Bossemeyer) will have different file formats

[8] https://www.moderntreasury.com/learn/bai2, EX2015.

[9] https://www.sepaforcorporates.com/swift-for-corporates/bai2-format-specification/, EX2016.

[10] https://blogs.sap.com/2015/10/20/ebs-how-to-interpret-a-bai2-file/, EX2017.

[11] https://www2.swift.com/knowledgecentre/products/Standards%20MT/publications, EX2018.

[12] https://www.iso20022.org/iso-20022-message-definitions, EX2019.

[13] https://achdevguide.nacha.org/ach-file-overview, EX2020.

depending on the vendor. Today, for example, Apple uses a propriety format[14] called PASS.[15] This is also not compatible with the bank file formats, and substantial file translation is required. In 2000 the situation was even more complicated. This was before Apple iPhone and Google Android became the dominant smart phone operating systems, there were even more diverse formats for digital wallets.[16, 17, 18, 19]

51. Not only does Bossemeyer not disclose merging of this data, but it would also take undue experimentation to merge, with no guarantee of success and

[14] https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/Creating.html, EX2021.

[15] https://developer.apple.com/library/archive/documentation/UserExperience/Reference/PassKit_Bundle/Chapters/Introduction.html, EX2022.

[16] https://www.usenix.org/legacy/event/ec98/full_papers/daswani/daswani.pdf, EX2023.

[17] https://www.gpayments.com/documents/GPayments_eWallet_Whitepaper.pdf, EX2024.

[18] https://www.maithean.com/products/wallet.html, EX2025.

[19] https://www.nytimes.com/1998/08/10/business/cybercash-s-lesson-in-web-survival.html, EX2026.

no benefit from attempting to do so. A similar issue exists with medical data (212, 214, 216 in Bossemeyer's Fig. 3). Medical data will be in different formats depending on the nature of the data. As a few examples: HL7 (Health Level Seven)[20] is used for clinical and administrative data, SDA (Summary Document Architecture)[21] is an InterSystems format used to represent patient data, EDI 837[22] is used for claim data. These disparate file types would also take undue experimentation to do so, with no guarantee of success and no benefit from attempting to do so. And neither the petition nor Dr. Zadok articulate any reason one would attempt to do so. It should be noted that HL7 was first introduced in 1987.[23] The EDI format originated in the 1990s.

52. Dr. Zadok also assumes that the only way to "use" the different pieces of information would have been to merge them. Based on my extensive experience and training with data, specifically with both the medical and financial data that is

[20] https://digitalhealth.folio3.com/blog/hl7-messages-examples/, EX2027.

[21] https://docs.intersystems.com/healthconnectlatest/csp/docbook/DocBook.UI.Page.cls?KEY=HXSDA_ch_about, EX2028.

[22] https://kasa-solutions.com/guide-to-the-837-file-format/, EX2029.

[23] https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/health-level-7, EX2030.

referenced in Bossemeyer, I strongly disagree with Dr. Zadok on this point. Data operations often make use of disparate pieces of information from different sources without merging or combining them. While merging can provide benefits in specific situations, it can also cause problems including duplicate data, inconsistent data, and inaccurate data.[24] Problems with merging data are well known in the art.[25, 26, 27, 28]

53. Dr. Zadok's last assumption is that merger of the different pieces of information, if it occurred, would constitute "reconstruction." But that could only be the case if those pieces of data were part of the same whole in the first place and were extracted to then later be merged. And, as I demonstrated above, Bossemeyer

[24] https://dataladder.com/merging-data-multiple-sources/, EX2031.

[25] https://www.tc.columbia.edu/media/centers-amp-labs/gsjp/gsjp-volume-pdfs/MergingMultipleandorDivergentDatasetsusingSPSS_AMethodReviewandTutorial.pdf, EX2032.

[26] https://libguides.princeton.edu/stata-merge-append, EX2033.

[27] Kadane, J. B. (2001). Some statistical problems in merging data files. Journal of Official Statistics, 17(3), 423 (https://www.scb.se/contentassets/ca21efb41fee47d293bbee5bf7be7fb3/some-statistical-problems-in-merging-data-files.pdf), EX 2034.

[28] https://nap.nationalacademies.org/read/24893/chapter/4, EX2035.

is entirely silent on the nature of the data before it is found in the portioned database server. Bossemeyer does not teach that these disparate pieces of information are ever part of a larger whole. Therefore, even if they were merged, there is no evidence that the result of that merger would constitute a "reconstruction." Rather, at most, one might consider such a merger to be the initial construction of a new dataset with multiple pieces of information.

54. Both Dr. Zadok and the petitioner rely on Bossemeyer's Figure 3 for the point that the central database server stores related information (e.g., medical information, financial information, etc.) in different areas of the partitioned memory, and that accessing these different areas may require different levels of security. Pet., 46, EX1003, ¶207. Again, all that Figure 3 indicates is that the merchant may access different types of information. It says nothing about what the merchant does with those different pieces of information when it obtains them. Bossemeyer provides neither a statement nor a suggestion that they are merged together, let alone that they are reconstructed into a combined form that they were previously in. And neither Dr. Zadok nor the petition provide any evidence that this is the case.

55. To agree with Dr. Zadok's opinion on "reconstruction," one would have to imagine that transactions couldn't occur without merging data, imagine that Bossemeyer has a merging step that it does not disclose, ignore the inherent difficulties in merging the various data types, ignore the possibility of data errors

when merging, and then assume that such merger would be the equivalent of the reconstruction of the ’987, even though Bossemeyer does not disclose any extraction of the data for the data to be reconstructed from.

56. For at least these reasons, I disagree with the petition and Dr. Zadok. Bossemeyer does not satisfy the required extraction or reconstruction elements of the different challenged claims, either explicitly, inherently, or via obviousness.

C. Absence of Reconstruction in Merenda

57. As also briefly explained above, Merenda concerns supporting direct email marketing and eCommerce. It has nothing to do with in-person transactions or smart cards, Bossemeyer’s focus. The concept of Merenda was for users to provide different types of information to a service and then dictate what entities could access that information. Those entities could then use that information in email marketing to customers. IBM never pursued it to a full patent, and it relates to an area simultaneously far afield from both the ’987 Patent and Bossemeyer.

58. In Merenda, the system presents the user with a web page with different fields for different types of information, such as name, address, and credit card number. EX1006, ¶¶23-24.

59. Web forms for obtaining data from the user are found in the two embodiments that Figures 2 and 3 illustrate, which illustrate Merenda’s two main embodiments, and the only ones that Dr. Zadok and the petition discuss.

60. The specification discussion of those two embodiments specifies that data enters the system through the web form. *See* Merenda EX1006 ¶26 (the Fig. 2 embodiment), ¶31 (the Fig. 3 embodiment).

61. In these two embodiments (Figures 2 and 3), either as the user enters each piece of information in a different field on the web form, or after the user has entered information in all the fields (Merenda doesn't specify), each individual piece of information is sent to a different location where it becomes part of a "data set."

62. The specification's description of the Figure 2 embodiment describes the data from each of the "public" fields being sent to be recorded as the "public data set," while data from each of the "private" fields is sent to be recorded as the "private data set." EX1006, ¶26.

63. The specification's description of the Figure 3 embodiment describes the same approach, with a slight variation that multiple public and private data sets are created: "Turning to FIG. 3 it is seen that a web form may generate a number of data sets 301 a-d…." EX1006, ¶31. That paragraph goes on to explain that "[e]ach time a new customer enters web form data, a record is created in the respective DB2 tables 302 a-d associated with the segmented data 301 a-d." The ***only*** records Merenda describes being created with respect to the Figure 3 embodiment are those separate ones in 302a-d; there's no original omnibus record with all the information.

64. In fact, nowhere, either generally with respect to Figure 1, or with respect to the Figures 2 or 3 embodiments, does Merenda disclose the full collection of information entered in the data fields being stored as, or constituting, a discrete "data set." As shown above, the individual pieces never go to a single repository for storage and processing. Instead, the different pieces of information initially go in different directions upon entry to be subsequently collected in separate data sets, or records. Paragraph 26 details this process: "Other items of information, such as the name, location, phone, e-mail, revenue, number of employees, may for our purposes, be designated as a single record 214 of private data elements 207 and as such will be stored separately in a private data set…." Only at that point are these "items of information" stored as actual records. Before that, they are independent "items of information."

65. The absence in Merenda of any discussion of storage of the full collection of information the user enters in the web form, such as in a table or in a particular database or software construct, is in marked contrast with Merenda's description of the way those individual items of information are later separately stored once they have been sent to the appropriate "data set." The Figure 2 embodiment, for example, shows the actual table structures of both the public data set (205) and the private data set (208), and these images are consistent with the specification's specification of DB2 databases. EX1006, Figs. 2, 3, ¶24. Similarly,

Figure 3 illustrating the second embodiment shows storage in what are expressly "DB2 Tables" at 302a-d. *See also* EX1006 ¶31. And Merenda later describes the data structure providing the aggregated public and private data to the merchant via an IBM Net. Data software product. EX1006, ¶32. IBM Net data is a scripting language for working with data sources such as DB2. DB2 is an IBM database. This dichotomy demonstrates that the initial items of information the user enters are never stored as a collective data set. In fact, the populated data tables do not yet exist when the customer enters data via the web form.

66. In one sentence in ¶24, Merenda does suggest that data could enter the system in some other manner than via a web form, such as via "surveys, transactional data, etc." EX1006. However, nowhere else does Merenda explain what those surveys/transactional data might include or look like or detail how ingestion of this data might occur. And nothing in the petition or Dr. Zadok's report seeks to fill in this absence with evidence or even supposition.

67. Once the information is entered and stored as different data sets, Merenda describes different "items of information"/"data elements" being "available" to different merchants for "view[ing]", based on the user's approval of which merchants could view which data sets. EX1006, ¶¶7, 9, 26, 29. That is its first embodiment. Merenda also describes a second embodiment, where different

records could be "collected and assembled into an output Web page" accessible through a URL. EX1006, ¶¶10, 30, 36.

68. The petition and Dr. Zadok look for "reconstruction" in Merenda. Both the petition and Dr. Zadok start by quoting from Merenda's ¶7 (describing its first embodiment), but all that paragraph states is that merchants may "access" stored information. Merenda goes on to describe what that might look like, "provid[ing] [the merchant] with the ability to view the particular consumers [*sic*] private data record." EX1006, ¶¶8-9, quoted by Dr. Zadok at ¶303. Getting access for viewing items of information is not "reconstruction." That's particularly true when what one is viewing data in a DB2 database populated with information that did not exist at the time that the user entered data on a web form, which is ***not*** structured as a DB2 database. DB2 databases are recorded and stored in a specific structure, which Merenda never describes doing with the full collection of information the user enters on the web form.

69. Both the petition and Dr. Zadok also quote from Merenda's ¶29, which is very similar to ¶¶7 and 9, and which also concerns Merenda's first embodiment. That paragraph states that "access to the data elements in the private data set may be made on an element-by-element basis, that is to say, that the merchant may be provided with access to certain select pieces of private data within the single [private] data record 214 [in Fig. 2]…." This statement suggests that anything

approaching reconstruction is ***not*** taking place; it describes merely providing access to single items of information, one at a time, not anything that is even analogous to reconstruction.

70. Both the petition and Dr. Zadok point to evidence about Merenda's second embodiment, particularly ¶¶10 and 30. In addition, Dr. Zadok's report additionally quotes from ¶36 and reproduces Figure 4, both also relating to the second embodiment. All of these parts of Merenda describe an embodiment where private and public data get aggregated in some fashion and made available for the merchant's viewing "by way of a customized Web page using a uniform resource locator (URL)." EX1006, ¶30; *see also* ¶¶10, 36, Fig. 4.

71. What both the petition and Dr. Zadok leave out of their discussion of the second embodiment, however, is Merenda's description of the nature and form of that "customized Web page" being presented to the merchant, or any discussion that that customized Web page constitutes a "reconstruction" according to the '987 Patent. That description from Merenda definitively establishes that there is no "reconstruction."

72. Under the petitioner's and Dr. Zadok's view, the user's filled-out Web form constitutes the original "data." I disagree, as I explain above, because those individual pieces of information are never recorded or stored as a cohesive whole. They instantly go to different places for storage as part of larger "data sets."

73. Even if one accepts the petition and Dr. Zadok's view of what constitutes the data, however, there can be no reconstruction according to the language of the claims of the '987 Patent.

74. All of the challenged independent claims of the '987 Patent require "reconstruction of ***said data***." EX1001, cls. 1, 10, 16, and 22 (emphasis added). "Said data" refers back to "data" in the claim, meaning the state the data started in before processing via extracting/parsing. In other words, what's being "reconstructed" must be, in whole or in part, the data as it originally existed before the extracting/parsing step.

75. This claim language is consistent with the '987 Patent specification's description of reconstruction, which makes clear that the reconstruction involves putting the data elements together in the form/structure in which they originally existed. *See, for example,* EX1001, Abstract, 7:3-9, 8:9-17.

76. Therefore, for the petition and Dr. Zadok to be right that there is "reconstruction of ***said data***," then this output, the "customized Web page" presented to the merchant must be, at least in part, identical to the web form initially submitted by the customer.

77. But Merenda's ¶32 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. It is an entirely new construct, with an entirely

different data structure: "Via the key-coded URL the merchant may access the query page 306 including the combined related records for John Doe joined by the logical relationship of the key value 123456789876. In a preferred embodiment the Web access to this combined table data may be accomplished by use of the IBM Net.Data software product." EX1006, ¶32. Thus, according to Merenda, this customized Web page presents data based on (i) a key-value relationship that did not exist at the time of data entry on the customer web form (ii) in a table form that it was not in at the time of data entry on the customer web form (iii) using (in the preferred embodiment) a software tool that was not employed at the time of data entry on the customer web form. Thus, 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.

78. For at least these reasons, Merenda does not teach "reconstruction of some or all of ***the data***."

D. Lack of Motivation to Combine Bossemeyer with Merenda

79. A person of ordinary skill in the art would not have been motivated to combine Bossemeyer and Merenda. I begin with affirmative reasons against such a combination and then turn to the five purported reasons asserted by the petition and Dr. Zadok.

i. A POSITA would not have sought to combine Bossemeyer and Merenda to reach the '987 claims because they are all in different technical fields.

80. The '987 Patent, Bossemeyer, and Merenda are from dramatically different technical fields, and a POSITA working with Bossemeyer as a foundation would not have been motivated to look for art in the far different field of Merenda for solutions to problems with Bossemeyer, as the petition and Dr. Zadok contend. Similarly, a POSITA working in the field of the '987 Patent would not have looked to Bossemeyer or Merenda for solutions to the problems addressed by the '987 claims.

81. As explained above, the field of the '987 Patent is data security for systems with large amounts of data, like email systems, browser programs, and telecommunications programs. EX1001, 1:14-22. More specifically, it concerns the processing, distribution, and secure storage of files/documents/data objects across telecommunications networks. EX1001, 1:14-22. Its prime focus is "securing data in a computer system." EX1001, 7:42. The PTO's lead Class for it is 709, "Electrical Computers and Digital Processing Systems: Multicomputer Data Transferring." Within that class, the USPTO subclass is 244 for "Centralized Controlling" for such information security systems. The USPTO describes that subclass as "subject matter wherein one computer selects the path used for data transfer by each of the other

computers."[29] I'd also note that the Petitioner's characterization of the field as "securing sensitive information" is so broad, encompassing such a wide array of technologies, as to be almost meaningless. For example, it would include encryption, dual-factor authentication, malware tools, firewall systems, tokenization (tap to pay) of financial information, blockchain, face ID, captcha, fingerprint scanners on computers, computer database technologies, cloud technologies, anti-surveillance technologies.

82. Bossemeyer's technical field is "smart card applications and, more particularly, to a network arrangement to provide access to an architecture that Supports a variety of advanced Smart card applications." EX1005, 1:7-11. That field involves technology for storing certain types of information on the card itself, technology for authenticating/authorizing reading the data on the card, reader technology for reading data on the card, and technology enabling the reader to communicate with remote networks and sending and obtaining information from those networks. EX1005, Fig. 1, 2:4-12, 3:53-58. The problems Bossemeyer seeks to address are specific to those types of technologies. Bossemeyer, for example, addresses ways of remotely storing information that could not be stored on the card

[29]https://web.archive.org/web/20080208014715/http://www.uspto.gov/web/patents/classification/uspc709/defs709.htm , EX2009

and then limiting the types of remote information returned to the reader depending on authorization. EX1005, 2:58-66. The USPTO's lead Class for Bossemeyer is 713, "Electrical Computers and Digital Processing Systems: Support." Its subclass within that Class is 201, "for computer network security in general or in combination with nominal cryptography.[30] Bossemeyer teaches a network connecting a smart card reader terminal through a phone network or the internet to a central storage server. EX1005, Figs. 1 and 2. It never considers hacking attacks, for example, and a successful hacker who gained access to Bossemeyer's central database server would have access to everything it stored.

83. Merenda's concerns World Wide Web eCommerce and targeted email marketing. Merenda seeks to provide a solution to the problem that "As the Internet evolves into the dominant commercial medium, merchants seeking to leverage data about Internet user's [sic] to better focus their marketing efforts must do so in a manner that respects the privacy interests of their intended customer." EX1006, ¶4. Merenda's USPTO primary Class is 707, "Data Processing: Database and File

[30] https://web.archive.org/web/20050422055224/http://www.uspto.gov/web/patents/classification/uspc713/defs713.htm, EX2010.

Management or Data Structures." Its subclass is 10, "distributed or remote access."[31] Its solution is a "program product for 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." EX1006, ¶2.

84. The patents' own descriptions as well as in the USPTO classifications make clear that they are in different fields. They support different applications (the '987 Patent's email systems, browser programs, and telecommunications programs. EX1001, 1:14-22) versus smart card applications (Bossemeyer) and eCommerce direct marketing (Merenda). Moreover, the only technical feature that Bossemeyer and Merenda have in common is that they store information in server memory.

85. It is also probable that, according to Petitioner's own definition of a POSITA for purposes of this proceeding, a POSITA working in the field of the '987 Patent would not have the requisite skills or technical experience to make changes to Bossemeyer's smart card system. Smart cards are a specialized field of technology (specialized storage on the card, specialized readers, etc.). Petitioner argues that a POSITA "would have had a bachelor's degree in computer science, computer engineering, electrical engineering, or equivalent, and approximately two years of

[31] https://web.archive.org/web/20041108063552/http://www.uspto.gov/web/patents/classification/uspc707/defs707.htm, EX2011.

experience working in the field of data storage systems and data security as of November 13, 2000." Pet., 8. It is quite possible for someone to complete a degree in computer science and not have any knowledge of smart cards. Again, as I noted above, smart cards were and remain a very specialized field that was not widely implemented or used during the relevant time frame.

86. It is not clear that a POSITA as identified by the petitioner would have the requisite knowledge about smart card technology to add Merenda to Bossemeyer to reach the claims of the '987 Patent, and the petition doesn't appear to try to establish that a POSITA would have. In the petitioner's description of a POSITA there is no mention of any knowledge of smart cards. And reviewing the curriculum at Stony Brook University, where Dr. Zadok teaches, it is quite clear that one can get a degree in computer science, computer engineering, or electrical engineering, with absolutely no training related to smart cards.[32] There is a passing mention of smart cards in the lecture notes for "System Security,"[33] however it is just a passing mention. I further note that the course "System Security" is a graduate course and

[32] https://www.cs.stonybrook.edu/students/Undergraduate-Studies/csecourses, EX2036.

[33] https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/resources/auth_notes.pdf, EX2037.

not one someone with a bachelor's degree in computer science would have taken.[34] A POSITA from the university that Dr. Zadok teaches at would not have the skills to make any modifications to any smart card.

ii. Petition's asserted motivations to combine.

87. The petition and Dr. Zadok assert five reasons for combining Bossemeyer and Merenda, but none withstands scrutiny.

88. The petition first asserts at page 52 that "use of known techniques according to known methods in the same way to yield predictable results." *See also* EX 1003, ¶315. That statement does not really suggest a motivation to combine two different references. The petition's real argument appears a couple of sentences later: "The combination would merely involve using Merenda's data parsing technique (parsing algorithm) in Bossemeyer's system according to methods for separating private and non-private elements within user data." Pet., 53. The petition then follows this statement with a long string cite to portions of Bossemeyer and Merenda without further explanation.

89. This first argument is effectively contending that it would have been easy to put these two references together and would merely have involved applying

[34] https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/lectures/L7_auth.pdf, EX2038.

known methods to achieve a predictable result. While I am not an expert on the law, from a technical expert perspective, this supposition does not seem like a motivation to combine two different references at a conceptual level. It's more a statement that if one thought of combining the two references, one might have a good chance of success (which I don't agree with, as detailed above). But it's not a reason to go and pick one piece of art out of a large field and put it with another.

90. A more specific problem with this contention is that it misunderstands what "parsing" in Merenda entails. I explained what Merenda's use of parsing refers to above: designating different types of information as either public or private. *Supra*, ¶¶60-65. Merenda's parsing does not relate to actually pulling individual pieces of data from a larger whole. In Merenda, items of information, such as name, address, social security number, *etc*. do end up in different public and private "data sets" after the customer enters those pieces of information in the web form, but those items of information are never part of a cohesive whole, and Merenda is silent on how each of those pieces of information ends up in a stored public or private data set after customer entry on the form. So, a combination that the petition and Dr. Zadok envision would not involve applying Merenda's "parsing" to Bossemeyer.

91. There's a similar problem with respect to what it assumes about Bossemeyer. As I explain above (*supra.*, ¶¶29, 53), Bossemeyer is silent about the nature and form of the data before it is found in the Central Database Server. All we

know from Bossemeyer is that different types of information are found in different partitioned areas of memory in that server. There's no evidence whatsoever that Bossemeyer begins with a collection of all these different types of information that need to be pulled apart/extracted in order to get into the appropriate places in the Central Database Server. As I note in paragraph 41 above, there are many ways for data to end up in partitioned memory that do not involve extraction.

92. In other words, the petition and Dr. Zadok are pointing to things not found in either Bossemeyer (an *ex ante* unpartitioned collection of all the different kinds of information) or Merenda (taking pieces of data out of a cohesive whole), and then contending that these things (that don't exist) could then be put together to achieve predictable results. But if neither exists in the first place, and they can't be put together, let alone with any predictability about results.

93. The petition's second purported motivation to combine (at p. 54) is that "Merenda identifies a known problem (e.g., controlling access to private information) and provides a solution to address the problem (e.g., parsing user data to extract the private elements and store private elements and non-private elements in separate memory stores)." This supposition also cannot qualify as a motivation to combine the two references.

94. As explained above with respect to the first purported motivation, this one is based on the same misunderstanding of what Merenda means by "parsing." Thus, it is flawed for that reason.

95. In addition, what the petition contends is the known problem, and its purported solution don't match up. In other words, the "solution" isn't a solution to the "problem" that the petition claims exists. The petition identifies the problem as "controlling access to private information" and the solution as "parsing user data to extract the private elements and store private elements and non-private elements in separate memory stores." Pet., 54. But even if Merenda's "parsing" did entail extraction, it wouldn't solve a need to "control access to private information." Merenda describes that control of access to the private data as an entirely separate step. For Merenda, the control step takes place by limiting which merchants can see the private data, regardless of how it got to storage or where it was stored. That happens as a result of the customer identifying which merchants may view its private information, and then providing those merchants either (embodiment 1) with that customer's key code to look up information in the private data set, or (embodiment 2) providing those merchants the key-coded URL to access information in the private data set. EX1006, ¶¶28-29, 35-36. Control over access is Merenda's limiting who receives access, which, again, is separate from storing different pieces of information in different places.

96. The petition's third asserted motivation to combine is that "Merenda's parsing technique to identify private elements within user data … would improve Bossemeyer's system for controlling access to sensitive/proprietary information." Pet., 55, EX 1003 ¶327. It contends that the addition would be controlling access "'at ***various levels of sophistication and granularity***.'" Pet., 55, quoting EX1006, ¶23 (emphasis in petition).

97. Merenda's method "for controlling access" that the petitioner is pointing to as being the source of this motivation to combine Merenda with Bossemeyer, however, wouldn't work with Bossemeyer. The reference to "various levels of sophistication and granularity" refers to what Merenda describes as either limiting access on an item-by-item basis, or limiting access if one seeks access to a combination of non-private items simultaneously. EX1006, ¶23.

98. The problem for the petitioner's position is that limiting access to only combinations of pieces of "public data," but not to the individual pieces of "public data" themselves would not be possible with Bossemeyer's smart card technology.

99. As already detailed above, the smart cards store "pointers" to particular areas of the partitioned memory. As part of a transaction, when a pointer stored on that smart card is invoked, the information stored in that particular area of portioned memory gets returned to the merchant. EX1005, 3:63-4:5.

100. I am not aware of a way to program into a smart card pointers to particular areas of the partitioned memory authorizing a merchant to access those areas, but preventing the triggering of those pointers and access to those areas were the merchant to request access to a particular combination of those areas to which it would have access individually. Bossemeyer acknowledges that the programmability of these smart cards is limited. EX1005, 2:66-3:2. For these reasons, it is unlikely that a POSITA at the time would have been able to do so.

101. Therefore, this third argument for a motivation to combine fails.

102. The petition's fourth purported motivation to combine is only briefly stated: "a POSITA would have been motivated to combine Bossemeyer with Merenda, because the combination would involve applying a known technique (e.g., using Merenda's parsing of user information and data entry) to a known device (e.g., Bossemeyer's network arrangement with a central database server storing user information), which was ready for improvement to yield predictable results." Pet., 56, EX1003, ¶332.

103. Again, this is not actually a motivation to combine. This is simply stating the opinion that one could combine them. My other points responding to the first purported motivation to combine would apply here as well. It is also based on a misunderstanding Merenda's "parsing." And Bossemeyer already details separate storage of public, limited access, and proprietary information and the conceptual

reasons for keeping them separate, so there would be no need for someone starting with Bossemeyer to look to Merenda. Neither the petitioner nor Dr. Zadok explain what benefit either Bossemeyer or Merenda would get from such a combination. A good analogy to the Petitioner's proposed combination of Bossemeyer and Merenda would be my attacking wheels to my coffee cup: I could do it, but it would provide no advantage and a POSITA would not be motivated to do so.

104. The petition's fifth and final purported motivation to combine is one that it contends is "express" in Merenda. Pet., 56, EX1003, ¶335. According to the petition, Merenda relates to the World Wide Web and eCommerce, which at the time was (and today continue to be) growing. The benefit of this growth, however, is "counterbalanced … [to some extent] by the inevitable loss of privacy" particularly as merchants "seek[] to leverage data about Internet user's [sic] to better focus their marketing efforts." Pet., 56, *quoting* Merenda EX1006, ¶¶3, 4. At the same time, Merenda saw "benefits … for respecting the privacy interests of the public." Pet., 57. In short, the petition is arguing that Merenda is about eCommerce, which can involve merchants getting direct access to some data for marketing purposes while still respecting some data privacy, and that these facts would motivate one to then combine Merenda with Bossemeyer. This is how the petition and Dr. Zadok frame the reason for the motivation to combine.

105. But it's not clear how these facts could establish a motivation to add Merenda to Bossemeyer. Bossemeyer is not concerned with the World Wide Web or eCommerce. It never refers to the World Wide Web. It never discusses targeted marketing to customers of the World Wide Web. Considerations about eCommerce, direct marketing, and the World Wide Web are wholly foreign and unrelated to the concerns that Bossemeyer addresses—improving smart cards.

106. It is true that Bossemeyer refers to the Internet, but the Internet is not the same as the World Wide Web, and Bossemeyer merely lists the former as a means for connecting the card reader with the central database server. The Internet is essentially a set of communication protocols that facilitate distributed communication and began as a Defense Advanced Research Projects Agency (DARPA) program in 1969.[35] The World Wide Web, on the other hand, is the invention of Tim Berners Lee working with CERN[36] and includes protocols such as Hyper Text Markup Language (HTML) and Hyper Text Transfer Protocol (HTTP). The World Wide Web is the deployment of content including eCommerce. A good analogy would be to think of the Internet as the interstate highway system, and the World Wide Web is one type of vehicle that traverses that highway. Bossemeyer's

[35] https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050, EX2039.

[36] https://www.slac.stanford.edu/history/earlyweb/history.shtml, EX2040.

only references to the Internet are to its use as a method of connecting merchants and their card readers to the central database server when the "Plain Old Telephone System" ("POTS") isn't used. EX1005, Fig. 2, 4:23-42.

107. Bossemeyer not only isn't concerned with facilitating data mining of customer information to allow for electronic direct marketing, but it also can't support it. In Bossemeyer, there's no way to reach the customer. The customer just has a smart card. He or she isn't using a computer to access the World Wide Web. So, he or she isn't getting emails or digital pop up ads on the screen.

108. What Bossemeyer is clear about, however, is the need to restrict information from getting to merchants unless it is necessary to conclude a transaction. EX1005, 5:6-15. In this sense, Bossemeyer is contrary to what the petition points to in Merenda. Bossemeyer wouldn't want merchants to get access to information for marketing purposes because Bossemeyer (i) out of concern for the privacy of certain kinds of data, only wants merchants to get the data pieces of information needed for the transaction, and (ii) can't support electronic marketing.

109. For these reasons, the fifth and final purported motivation to combine fails as well.

IX. CONCLUSIONS

110. Upon completing my analysis, I have reached the following conclusions. Bossemeyer fails to disclose at least two claim elements found in every

challenged claim, the "extracting/parsing" element and the "reconstruction" element. Merenda fails to disclose at least the "reconstruction" element. Even if Merenda discloses claim elements that are missing from Bossemeyer, Petitioner failed to establish a motivation to combine Merenda with Bossemeyer. A POSITA, as defined by the petitioner would likely not have looked to Merenda to combine with Bossemeyer or had the skills to combine Bossemeyer with Merenda. Nor would a person of skill in the art have had a reason to combine elements from Merenda with elements from Bossemeyer in the first place.

Dated: September 12, 2023



Dr. William C. Easttom II

APPENDIX A

MATERIALS REVIEWED

The petition for IPR2023-00969 and all exhibits to that petition

The expert declaration of Dr. Erez Zadok, EX1003 and all exhibits to that declaration

U.S. Patent No. 7,349,987

U.S. Patent No. 7,010,701 (Bossemeyer)

U.S. Publication No. 2004/0148290 (Merenda)

U.S. Patent No. 6,845,488 (Chaganti)

U.S. Publication No. 2004/0199765 ("Kohane)

USPTO Patent Classification Code Definitions – Class 707 – https://web.archive.org/web/20041108063552/http://www.uspto.gov/web/patents/classification/uspc707/defs707.htm

USPTO Patent Classification Code Definitions – Class 709 – https://web.archive.org/web/20080208014715/http://www.uspto.gov/web/patents/classification/uspc709/defs709.htm

USPTO Patent Classification Code Definitions – Class 713 – https://web.archive.org/web/20050422055224/http://www.uspto.gov/web/patents/classification/uspc713/defs713.htm.

McClannan, Keith, *Implementing Smart Cards Into the Air Force Reserve*, Air Command and Staff College, April 2001 - https://apps.dtic.mil/sti/pdfs/ADA406328.pdf

Posey, Brien, *All about partitions: The right FAT can save your waste*, Daily Tech Insider, Sep. 2000 - https://www.techrepublic.com/article/all-about-partitions-the-right-fat-can-save-your-waste

Walker, Martin, *Splitting Your PC Data Across Multiple Drives & Partitions*, Sound on Sound, Aug. 2000 -

https://www.soundonsound.com/techniques/splitting-your-pc-data-across-multiple-drives-partitions

Prentice Hall's Illustrated Dictionary of Computing, 3rd Edition, 1998

BAI2, Modern Treasury Corp., – https://www.moderntreasury.com/learn/bai2

BAI2 Format Specification, SEPA for Corporates, Jan. 2015 – https://www.sepaforcorporates.com/swift-for-corporates/bai2-format-specification/

Maheshwari, Ajay*, EBS – How to interpret a BAI2 file*, SAP, Oct. 2015 – https://blogs.sap.com/2015/10/20/ebs-how-to-interpret-a-bai2-file/

Standards MT, Swift, 2023 - https://www2.swift.com/knowledgecentre/products/Standards%20MT/publications

ISO 20022 Message Definitions, ISO, Sep. 2010 – https://www.iso20022.org/iso-20022-message-definitions

ACH Guide for Developers, Nacha, - https://achdevguide.nacha.org/ach-file-overview

Pass Design and Creation, Wallet Developer Guide, Jan. 2018 – https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/PassKit_PG/Creating.html

About Pass Files, Apple Inc., Nov. 2017 – https://developer.apple.com/library/archive/documentation/UserExperience/Reference/PassKit_Bundle/Chapters/Introduction.html

Daswani, Neil et. al., *SWAPEROO: A Simple Wallet Architecture for Payments, Exchanges, Refunds, and Other Operations*, USENIX Workshop, Aug. 1998 – https://www.usenix.org/legacy/event/ec98/full_papers/daswani/daswani.pdf

Clark, Brent, *Electronic Wallets: Past, Present, and Future*, GPayments, 2001 – https://www.gpayments.com/documents/GPayments_eWallet_Whitepaper.pdf

NetPay Wallet, Maithean, - https://www.maithean.com/products/wallet.html

Wayner, Peter, *Cyberchas's Lesson in Web Survival*, The New York Times, Aug. 1998 - https://www.nytimes.com/1998/08/10/business/cybercash-s-lesson-in-web-survival.html

HL7 Messages Examples – Complete Guide 2023, folio3 Software Inc., - https://digitalhealth.folio3.com/blog/hl7-messages-examples/

About SDA, InterSystems, 2023 – https://docs.intersystems.com/healthconnectlatest/csp/docbook/DocBook.UI.Page.cls?KEY=HXSDA_ch_about

Guide to the 837 File Format, Kasa Solutions, - https://kasa-solutions.com/guide-to-the-837-file-format/

Denecke, Kerstin, *Biomedical Standards and Open Health Data*, Science Direct, 2021 – https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/health-level-7

Ibarrera, *Merging data from multiple sources*, Data Ladder, Nov. 2021 – https://dataladder.com/merging-data-multiple-sources/

Audette, Lillian M. et. al., *Merging Multiple and/or Divergent Datasets using SPSS: A Method Review and Tutorial*, Graduate Student Journal of Psychology 2022, Vol. 19, 2022 – https://www.tc.columbia.edu/media/centers-amp-labs/gsjp/gsjp-volume-pdfs/MergingMultipleandorDivergentDatasetsusingSPSS_AMethodReviewandTutorial.pdf

Al, Muhammad et. at., *Merge and Append Using Stata: How to Merge and Append Datasets*, Princeton University, May 2023 - https://libguides.princeton.edu/stata-merge-append

Kadane, Joseph B., *Some Statistical Problems in Merging Data Files*, Journal of Official Statistics, Vol. 17, No. 3, 2001 - https://www.scb.se/contentassets/ca21efb41fee47d293bbee5bf7be7fb3/some-statistical-problems-in-merging-data-files.pdf

Groves, Robert M. et. al., *Federal Statistics, Multiple Data Sources, And Privacy Protection*, The National Academies Press, 2017 - https://nap.nationalacademies.org/read/24893/chapter/4

Department of Computer Science CSE Courses, Stony Brook University – https://www.cs.stonybrook.edu/students/Undergraduate-Studies/csecourses

Lecture Notes for Chapter 3 System Security, Stony Brook University - https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/resources/auth_notes.pdf.

Sekar, R., *CSE509 - Computer System Security*, Stony Brook University – https://www3.cs.stonybrook.edu/~amione/CSE509_Course/materials/lectures/L7_auth.pdf

A Brief History of NSF and the Internet, National Science Foundation, Aug. 2003 – https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

Lee, Tim Berners, *Early Chronology and Documents*, Stanford University, 2020 - https://www.slac.stanford.edu/history/earlyweb/history.shtml