

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,
Petitioner,
v.
FORTINET, INC.,
Patent Owner.

PTAB Case No. IPR2023-00458

Patent No. 9,280,678 B2

**PETITIONER NETSKOPE, INC.'S REPLY TO PATENT OWNER'S
RESPONSE TO PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. PATENT NO. 9,280,678 B2**

TABLE OF CONTENTS

Page

UPDATED EXHIBIT LIST	III
I. INTRODUCTION	1
II. CLAIM CONSTRUCTION	1
A. “Namespace” simply means “the set of names available for naming things.”	1
B. “Creating” and “configuring” are not part of encrypting the file content.	2
C. The Board has already rejected PO’s “single policy” interpretation of “policy.”	4
III. GROUNDS 1-3.....	6
A. Claims 1/16: Cidon in view of Shikfa rendered obvious “creating namespaces” and “configuring the namespaces.”	6
1. Cidon’s creating identifiers constituted creating namespaces.....	6
2. Cidon’s identifiers were created as part of encrypting the content to produce a searchable encrypted file.....	9
3. Shikfa’s mapping of keywords to identifiers in an index constituted “configuring the namespaces.”	11
B. Claim 1/16: A POSITA would have been motivated to combine Cidon and Herrmann with Shikfa.	13
C. Claims 1/16: The Cidon combination disclosed or rendered obvious a “policy for managing access to and processing a file to be stored on cloud platforms.”	14
1. Cidon’s policy was assigned to a “user.”.....	14
2. Cidon’s policy met the “processing” limitation.....	17
3. Cidon’s policy did govern access management.....	17
D. Claims 1/16: Cidon disclosed or rendered obvious “storing, by the gateway device” (claim 1) and “a storage module” for storing (claim 16) “the searchable encrypted file on the one or more cloud	

TABLE OF CONTENTS

	Page
platforms based on the policy.”	18
E. Claims 11/25: Cidon disclosed or rendered obvious storing a file “across two or more cloud platforms.	19
F. Claim 14: Cidon disclosed or rendered obvious a policy that defines “one or more authorized locations to which the file may be stored.20	20
G. PO did not separately dispute Grounds 2 and 3	20
IV. GROUND 4: AURADKAR, CHIUEH, AND CHAMBERS RENDERED CLAIMS 1-3, 8-19, 21-27 OBVIOUS.....	20
A. Claims 1/16: Auradkar in view of Chiueh rendered obvious “creating namespaces” or configuring the namespaces ... such that content of the file is encrypted in a manner that makes it searchable.”	20
1. Creating identifiers constituted creating namespaces.....	21
2. Chiueh’s mapping of keywords to document identifiers in an index constituted “configuring the namespaces.”	26
3. A POSITA would have been motivated to combine Auradkar, Chambers, and Chiueh.....	30
B. Claims 1/16: Auradkar disclosed “cryptographic key information defined by the policy.”	31
C. Claims 1/16: Auradkar disclosed a policy for “processing of a file to be uploaded on a cloud.”	32
V. GROUND 5: AURADKAR AND INOUE RENDERED OBVIOUS CLAIM 6.....	32
VI. CONCLUSION.....	33

UPDATED EXHIBIT LIST

Exhibit	Description
Ex. 1001	U.S. Patent No. 9,280,678 to Redberg (“the ’678 Patent”)
Ex. 1002	Supporting Declaration of Dr. Wenke Lee (“Lee”)
Ex. 1003	File History of U.S. Patent No. 9,280,678
Ex. 1004	U.S. Patent Application Publication No. 2014/0013112 (“Cidon”)
Ex. 1005	U.S. Patent Application Publication No. 2003/0055994 (“Herrmann”)
Ex. 1006	U.S. Patent Application Publication No. 2014/0359282 (“Shikfa”)
Ex. 1007	U.S. Patent Application Publication No. 2005/0010593 (“Fellenstein”)
Ex. 1008	U.S. Patent No. 6,622,248 (“Hirai”)
Ex. 1009	U.S. Patent Application Publication No. 2011/0119481 (“Auradkar”)
Ex. 1010	U.S. Patent Application Publication No. 2014/0068030 (“Chambers”)
Ex. 1011	U.S. Patent Application Publication No. 2013/0159694 (“Chiueh”)
Ex. 1012	U.S. Patent Application Publication No. 2003/0063321 (“Inoue”)
Ex. 1013	U.S. Patent Application Publication No. 2002/0099666 (Dryer)
Ex. 1014	Dictionary of Computer and Internet Terms, Tenth Edition (2009)
Ex. 1015	U.S. Patent Application Publication No. 2011/0145594 (“Ex. 1015”)
Ex. 1016	U.S. Patent Application Publication No. 2009/0300351 (“Ex. 1016”)
Ex. 1017	U.S. Patent Application Publication No. 2008/0069480 (“Ex. 1017”)
Ex. 1018	Song, D. X., Wagner, D., & Perrig, A. (2000, May). Practical techniques for searches on encrypted data. In Proceeding 2000 IEEE symposium on security and privacy. S&P 2000 (pp.44-55) (“Song”)

Exhibit	Description
Ex. 1019	Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. (2004, June). Order preserving encryption for numeric data. In Proceedings of the 2004 ACM SIGMOD international conference on Management of data (pp.563-574) (“Agrawal”)
Ex. 1020	Adya, A., Bolosky, W. J., Castro, M., Cermak, G., Chaiken, R., Douceur, J. R., Howell, J., Lorch, J. R., Theimer, M., and Wattenhofer, R. P. 2002. Farsite: federated, available, and reliable storage for an incompletely trusted environment. SIGOPS Oper. Syst. Rev. 36, SI (Dec. 2002), 1-14 (“Ex. 1020”)
Ex. 1021	Mika, P., & Potter, T. (2012). Metadata Statistics for a Large Web Corpus. LDOW, 937 (“Ex. 1021”)
Ex. 1022	Microsoft Computer Dictionary, Fifth Edition (2002)
Ex. 1023	Balakrishnan, H., Lakshminarayanan, K., Ratnasamy, S., Shenker, S., Stoica, I., & Walfish, M. (2004). A layered naming architecture for the Internet. ACM SIGCOMM Computer Communication Review, 34(4), 343-352 (“Ex. 1023”)
Ex. 1024	Declaration of Andrew N. Klein in Support of <i>Pro Hac Vice</i> Admission
Ex. 1025	Deposition Transcript of Dr. John Richard Black (“Black Tr.”)
Ex. 1026	Supplemental Declaration of Dr. Wenke Lee (“Lee Suppl.”)
Ex. 1027	The Merriam-Webster Dictionary, Sixth Edition, 2004

I. INTRODUCTION

Patent Owner fails to rebut Petitioner's showing that the challenged claims of U.S. Patent No. 9,280,678 ("the '678 patent") are obvious. Instead, PO's arguments largely hinge on these misconceptions:

1. "Namespace" requiring a predefined set of names available within a particular context;
2. "Creating" and "configuring" namespaces being part of encrypting content of the file ;
3. "Configuring" namespaces requiring modifying the namespaces;
4. A "policy" being a "single policy."
5. Teaching-away of Petitioner's combinations.

As explained below, none of these assertions are supported by the evidence.

II. CLAIM CONSTRUCTION

A. "Namespace" simply means "the set of names available for naming things."

The '678 patent does not describe what namespaces are. *See generally* '678 Patent; Black Tr., 39:17-20. The plain meaning of "namespace" should be "the set of names available for naming things." Lee, ¶101; Ex. 1014 (Dictionary of Computer and Internet Terms).

PO mischaracterizes Dr. Lee's testimony, arguing that a POSITA would not consider names created while producing searchable encrypted content (e.g., "1234") as namespaces. POR, 18. But Dr. Lee testifies that a namespace can be any number within a range (e.g., 0 to $2^{128}-1$), explaining "1234" is not just a member within a

namespace; it is one. Lee Decl., ¶42; *see also* Ex. 1023, 344.

Moreover, Dr. Lee disagrees with PO’s proposed meaning of “namespace” as “a set of names available *within a particular context*.”¹ POR, 18. Notably, “within a particular context” is vague and encapsulates practically anything. Dr. Lee explains that namespaces’ main function is to uniquely identify objects by their names within the context of the namespace, not constraining the names to a *particular* context. Lee, ¶42; Lee Tr. 39:6-40:1. Instead, namespaces can be defined in various ways (e.g., individual identifiers) if they enable unique identification. *Id.*

Dr. Lee’s testimony also undermines PO’s position of “namespace” being limited to predefined names. POR, 18-19. Dr. Lee explains that the “*documents*” *namespace provides a context* within which the “foo” file is unique. Lee Tr., 38:13-23; *see also id.*, 37:22-38:2 (describing that the “documents” namespace is the scope of the files contained in the “documents” directory).

B. “Creating” and “configuring” are not part of encrypting the file content.

The ’678 patent is clear that “creating” and “configuring” namespaces are *not* part of encrypting content of the file. Notably, claim 1 recites encrypting content of the file *to produce a searchable encrypted file by* performing operations:

¹ All **bold** or *italic* emphases herein are added by Petitioner unless otherwise specified.

- (a) dividing the file into a plurality of chunks;
- (b) creating namespaces for one or more of the plurality of chunks; and
- (c) configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.

'678 Patent, 19:62-20:3. These operations describe how *the encrypted searchable file* is produced and not the specific steps contained within the “encrypting” operation. Lee Suppl., ¶2.

PO's argument also contradicts the example in Appendix A of the '678 patent, where the Encryption step of the “Dragonfruit” solution contains nothing beyond “encrypting each record one by one” to produce a cipher text vector. '678 patent, Appendix A, Section IV; Lee Suppl., ¶3.

Tellingly, PO and its expert contradict their own position. For example, PO and Dr. Black contend “*policies therefore create a namespace* that defines the naming convention for the file chunks.” POR, 20; Ex. 2003, ¶ 71. But creating a namespace by defining a naming convention occurs *prior* to encrypting the file content. That contradicts PO's later statements that Cidon's set of SHA-2 signatures were defined in advance of encryption and therefore are not namespaces. POR, 22; Lee Suppl., ¶4.

PO separately contends “*naming the folder with the encrypted filename* and storing the file chunks in that folder *creates a namespace* scope for the file chunks,”

but naming the folder is not part of *encrypting the file content*. POR, 20; Ex. 2003, ¶ 71; Lee Suppl., ¶¶5-6; Black Tr. 54:15-17 (“I agree with you if you’re saying that the contents of the file, if you encrypt that, that’s not influencing directly the filename.”).

C. The Board has already rejected PO’s “single policy” interpretation.

As it did in its institution decision, the Board here should again reject PO’s attempt to limit “policy” to a “single policy.” Inst. Dec., 18-19.

The ’678 claims merely recite a “policy,” not a “single policy.” Indeed, the ’678 expressly explains that a policy can include “sub-policies.” ’678 Patent, 9:40-46; Lee Suppl., ¶7. PO provides no basis to contradict the express teachings of the patent.

PO’s approach is also legally flawed. “As a general rule, the words ‘a’ or ‘an’ in a patent claim carry the meaning of ‘one or more.’” *TiVo, Inc. v. EchoStar Commc’ns Corp.*, 516 F.3d 1290, 1303 (Fed. Cir 2008). “The exceptions to this rule are *extremely limited*: a patentee must evince a *clear intent* to limit ‘a’ or ‘an’ to ‘one.’” *Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1342 (Fed. Cir. 2008). Here, PO has not even tried to demonstrate such “intent” and, as noted above, the ’678 patent expressly evidences the opposite by contemplating multiple sub-policies.

Moreover, PO’s analogy between microprocessors and policies (POR, 38) is

flawed due to the fundamentally different technology in *Salazar v. AT&T Mobility LLC*, 64 F.4th 1311 (Fed. Cir. 2023). Unlike the **hardware** microprocessors in *Salazar*, here a “policy”—software rules—comprises multiple policies or sub-policies, addressing **different** functions, like defining “access rights” and “cryptographic key information.” ’678 Patent, 19:61-63. As the Board noted on institution, the ’678 Patent itself describes the policy for “defin[ing] access rights, storage diversity requirements and a type of encryption” being different from the policy for defining “cryptographic key information.” Inst. Decs., 18 (citing ’678 Patent at 2:18-22). PO’s own expert, Dr. Black, also admits that a policy comprises “**distinct** sections,” each specifying a particular function. Black Tr., 10:12-11:14, 12:1-3, 13:9-14:16. This aspect of policy management unequivocally shows a “policy” can be a collection of policies.

Similarly, as the Board found, Cidon’s policy contained several components that controlled multiple aspects like file access, processing, encryption, and management. Inst. Decs., 19. Therefore, Cidon’s policy managed file processing and also defined access rights of users, cryptographic key information, and file storage, consistent with *Salazar*.

Further, PO’s reliance on *TiVo* is misplaced. POR, 38-39. In *TiVo*, the court emphasized the specific sequence of operations—namely, converting a signal into an MPEG stream, parsing this stream into components, and later reassembling these

components back into a single stream. *TiVo, Inc. v. EchoStar Commc'ns Corp.*, 516 F.3d 1290, 1303-4 (Fed. Cir. 2008). This sequence established a cyclical relationship between the initial and final forms of the stream. *Id.* By contrast, the “policy” here is not tied to a process that breaks down a single policy into constituent parts only to reassemble them into their original form.

III. GROUNDS 1-3

A. Claims 1/16: Cidon and Shikfa rendered creating and configuring namespaces obvious.

1. Cidon’s creating identifiers constituted creating namespaces.

The ’678 patent mentions “namespaces” only four times, without defining them or explaining how to create them. *See* ’678 Patent, 6:44-47, 9:19-26, 10:11-16, FIG. 3A²; Black Tr., 42:20-43:2. Namespace creation does not require defining a range of names as PO argues.³ POR, 18; Pet., 11-12; Lee, ¶42. This can include simple cases, such as naming files (or file chunks) with specific identifiers. In fact, claim 1 recites “creating namespaces *for one* or more of the plurality of chunks,”

² Step 306 states “Encrypt each File Chunk...such that Namespace is Created,” without any corresponding textual explanation.

³ Dr. Black confirmed that namespaces creation does not require enumerating all members of the namespaces. Black Tr., 68:5-10.

suggesting it suffices to create a namespace for *one* file chunk and does not require creating a range of names or values. Lee Suppl., ¶¶8.

Cidon disclosed creating namespaces because it described generating unique identifiers for file segments (chunks) based on their contents using SHA-2 signature computation. Cidon, ¶¶305, 383, FIG. 13.

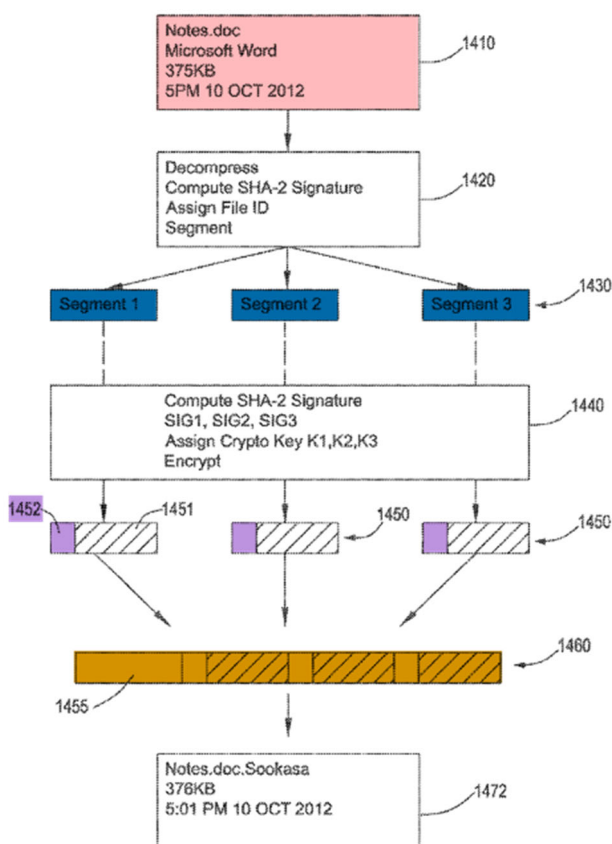


FIG. 13 (Annotated)

Cidon, FIG. 13.

A POSITA would have understood that the SHA-2 algorithm produces a fixed-length hash (256-bit output). Lee Suppl., ¶¶9-10. This fixed-length hash assigned to an identifier has a format similar to that of other exemplary namespaces

in the field, like number “1234” within 0 to $2^{256}-1$. *Id.*; Ex. 1023, 344. Therefore, Cidon’s use of SHA-2 to generate the identifier(s) for the file chunk(s) constituted creating namespaces for the file chunks. Lee Suppl., ¶10.

Moreover, even under PO’s proposed construction, Cidon’s identifiers still constituted “namespaces,” because they were unique within the system’s context (e.g., encrypted file 1460), falling within a prescribed range (e.g., a 256-bit value) and uniquely identifying an individual segment. Cidon’s namespaces were created when identifiers 1452 were assigned to file segments 1451, 1450, thus creating a unique set of names within the context of encrypted file 1460. Cidon, FIG. 13.

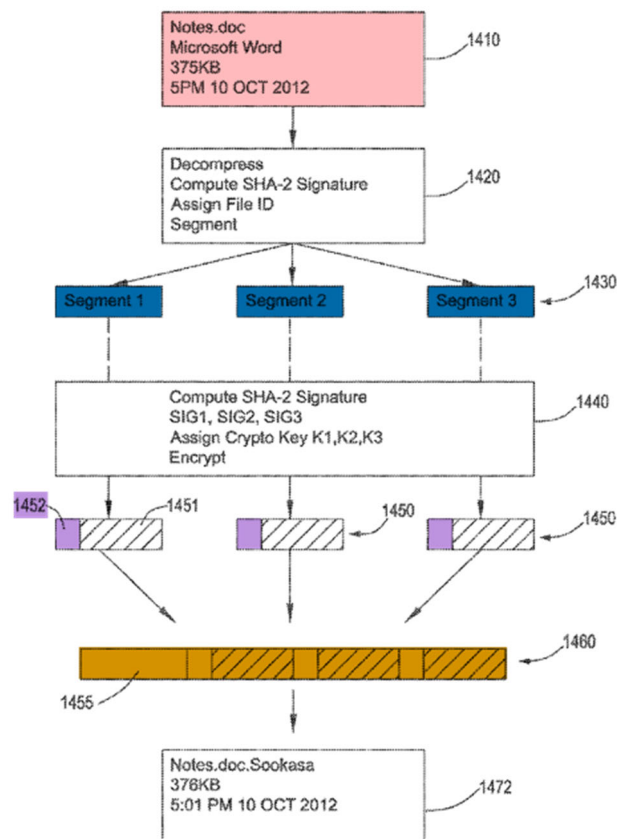


FIG. 13 (Annotated)

2. Cidon’s identifiers were created as part of encrypting the content to produce a searchable encrypted file.

PO also argues that Cidon did not “create the namespace during the encryption process because it was created in advance.” POR, 24. This argument fails because as explained in Section II.B, the claims recite that the “creating” step is part of producing searchable encrypted content, i.e., exactly what Cidon taught. *See* Cidon, ¶¶305, 383, FIG. 13.

However, even under PO’s proposed construction, Cidon’s creating and assigning identifiers were part of the encryption process. Notably, Cidon’s using the SHA-2 algorithm to produce hashes that resulted in creating namespaces were carried out as part of the encryption process. Lee Suppl., ¶11. Cidon’s operations align closely with the ’678 patent. *Compare* ’678 Patent, FIG. 3A *with* Cidon, FIG. 13.

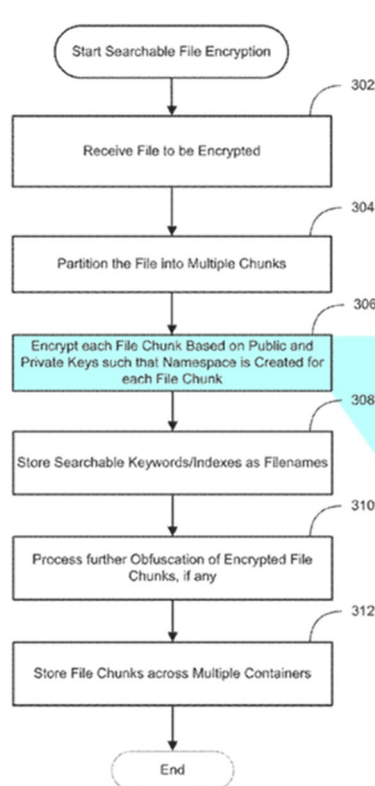


Fig. 3A (Annotated)

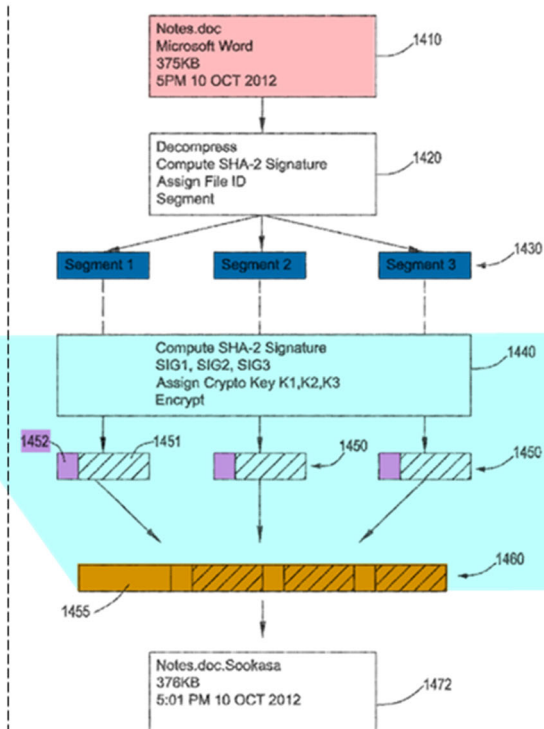


FIG. 13 (Annotated)

'678 Patent, FIG. 3A

Cidon, FIG. 13.

In Cidon, when content was encrypted (1450), unique identifiers (1452) were produced and assigned to file segments, thereby creating namespaces for them. These namespaces were thus created as part of encryption. Moreover, while the range of possible SHA-2 signatures could be predefined as POR argues at 24, the claims do not preclude using a pre-assigned range of numbers for namespace creation. Indeed, the '678 patent provides no explanations for creating namespaces. *See* §II.A.

3. Shikfa’s mapping of keywords to identifiers constituted “configuring the namespaces.”

PO first argues that Shikfa’s mapping keywords to identifiers to encrypted documents does not “configur[e] the namespaces” because identifiers are not namespaces. POR, 25. However, this argument fails because Shikfa’s identifiers, like Cidon’s identifiers, constituted namespaces. *See* §III.A.1.

Before addressing PO’s remaining arguments, it is important to note that the ’678 patent’s only clear reference to configuring namespaces is in dependent claim 6, which recites “configuring the namespace comprises storing content of the file as filenames.” ’678 patent, 20:20-22; *see also id.*, 12:7-9. But the scope of the “configuring” step in the independent claims is broader than the specific recitations in claim 6 based on claim differentiation. Thus, PO’s alleged “novel process” involving using the encrypted keywords as filenames in namespace configuration (POR, 28)⁴ cannot be imported into independent claims that lack those limitations. The incorporation of search terms into filenames is one non-exclusive example of the “configuring.” ’678 Patent, 2:52-54 (“an exemplary flow chart”; “an embodiment”), Figure 3A; Black Tr., 19:17-22 (“It’s an embodiment.”), 85:13-20.

A POSITA would understand that “configuring” encompasses any of arrangement, use, or integration in “a particular way” to achieve specific

⁴ As shown in Grounds 2 and 5, claim 6 is also invalid.

functionality. Ex. 1027 (defining “configure” as “to set up for operation esp. in a particular way”); Lee Suppl., ¶12. Shikfa mapped its identifiers to keywords in indexes in a particular way to reference encrypted file chunks, and thus **configured** those identifiers to make the encrypted content searchable. Lee Suppl., ¶12.

PO further argues that Shikfa’s use of identifiers bears no relationship to encryption. POR, 27-28. But, as explained in Section II.B, the claims do not require “configuring” to be part of encrypting content of the file. Additionally, Petition’s invalidity grounds combine Shikfa with Cidon; in the combination, the namespaces configuration is conducted as part of the encryption process. Pet., 40-43; *see also* §III.A.2. Thus, this limitation is satisfied even under PO’s improper construction.

PO asserts that Shikfa’s index was not configured as part of content encryption because it is created before a document is encrypted. POR, 27 (citing Shikfa ¶29). But this mischaracterizes Shikfa, wherein the very next sentence explains that each index includes a pointer to the encrypted document, which could only be done **after, or during the** encryption. Shikfa, ¶ 29.

Additionally, Dr. Lee’s testimony does not support PO’s assertion that the “manner in which the file is encrypted is...‘orthogonal’ to **the use of identifiers.**” POR, 27. Instead, Dr. Lee used terms “independent” and “orthogonal” to describe flexibility in choosing encryption mechanisms for encrypting documents and indexes, not a separation of indexing and encryption functionalities. Lee Tr., 136:13-

137:7.

B. Claim 1/16: A POSITA would have been motivated to combine Cidon and Herrmann with Shikfa.

PO contends that a POSITA would not have “incorporated Herrmann’s gateway server into the modified system (because Shikfa already discloses one).” POR, 29. However, PO overlooks the benefits of adding Herrmann’s gateway beyond Shikfa. Pet., 22, 27; Lee, ¶¶68-69, 80. Indeed, the searchable encryption mechanism provided by Shikfa is what a POSITA would have integrated with Cidon’s system, independent of the hardware or server architecture Shikfa used. *Id.*

Moreover, PO appears to argue for a lack of motivation because of Shikfa’s client-side encryption. POR, 29. But the Board already rejected this argument for “attack[ing] the references individually.” Inst. Dec., 24. Indeed, Shikfa’s client-side encryption did not preclude incorporating a gateway with a similar encryption functionality in the Cidon-Herrmann combination. Pet., 43-44; Lee, ¶¶ 105-106.

PO’s alleged concern of privacy is misplaced because in the Cidon-Herrmann-Shikfa combination, the gateway would be an entrusted party controlled by the data-protecting organization. PO again twists Dr. Lee’s testimony regarding encryption and key negotiation process. POR, 29-30. Dr. Lee stresses that encryption effectiveness depends more on implementation strategy, rather than the physical location of encryption. Lee Tr., 80:4-9, 82:20-24.

Shikfa also did not teach away the gateway-side encryption because it does

not “criticize, discredit, or otherwise discourage investigation into’ the claimed invention.” *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017) (citation omitted). Rather, Shikfa described broader principles of searchable encryption applicable to various system configurations, including those where a gateway device performs encryption. Pet., 45; Lee, ¶107.

C. Claims 1/16: The Cidon combination disclosed or rendered obvious a “policy for managing access to and processing a file to be stored on cloud platforms.”

1. Cidon’s policy was assigned to a “user.”

As an initial matter, PO’s assertion that policies must be assigned solely to individuals (POR, 31) contradicts the ’678 patent. The ’678 patent expressly states that the terms “users” and “clients” are used interchangeably. ’678 Patent, 8:5-7. These clients 102 are “operatively and communicatively coupled to each other through a local area network (LAN) 104,” and include a “data agent” software module. ’678 patent, 6:55-7:4, FIG. 1 (annotated below). Thus, “clients 102” can be client devices.

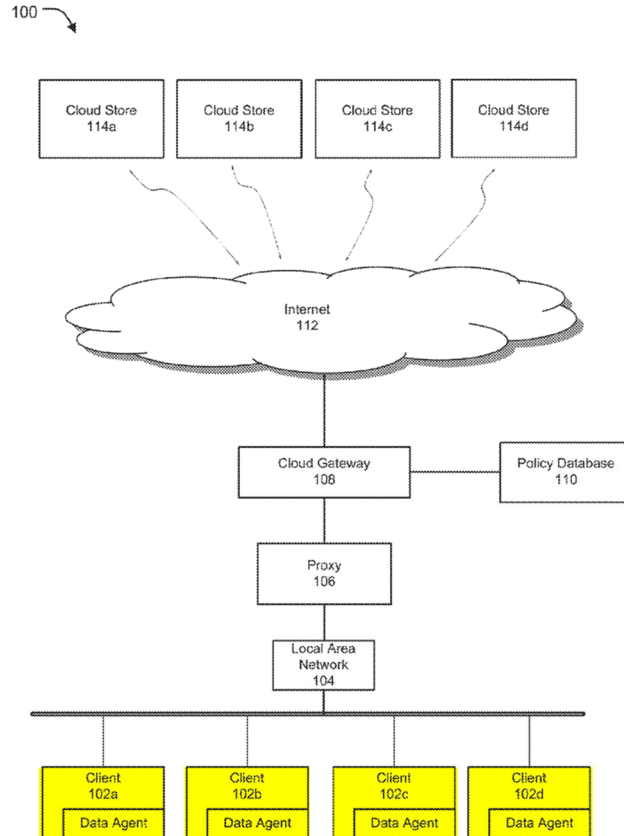


Fig. 1(Annotated)

'678 Patent, FIG. 1.

Regardless, contrary to PO's contention (POR, 31), Cidon's policy was also assigned to a user or a group of users. Pet., 25; Cidon, ¶108. The '678 patent does not prohibit or disavow assigning policies to a group of users (Black Tr., 17:5-7), and in fact claim 23 expressly recites that "the policy is implemented for a group of users." '678 patent, 22:12-13.

Additionally, PO's interpretation of Cidon's policy as a "specific file" overlooks the broader context. POR, 32. Notably, Cidon's policy includes access policies, encryption policies, and policies for handling files. Cidon, ¶¶102, 108, 146,

206-217, 227; *see also* Inst. Dec., 19 (discussing various functionalities of Cidon’s policy). Similarly, as explained earlier, the ’678 policy includes multiple policies or sub-policies, each addressing a **different** function. Section II.C. Put differently, Cidon’s encryption policy, like the ’678 patent’s sub-policies, was part of a comprehensive policy that governed file processing and access relating to users. Pet., 29, 33, 48-49; Cidon, ¶¶102, 108, 208-209, 214-215, 324, 326.

Further, PO’s argument that Cidon’s encryption policies were solely defined on documents but not assigned to users (POR, 32) overlooks the flexibility of Cidon’s policy framework at the user level. Notably, Cidon’s policy specified **access** and **sharing** permissions, **copy** control, and encryption, which suggests the policy was user-specific. *Id.*, ¶¶207-213; Lee Suppl., ¶13. Indeed, Cidon further described that upon detecting a policy violation, its system alerted **users** (not administrators) and allowed them to approve the violation or change the policy if needed, confirming Cidon’s policy was user-specific. *Id.*, ¶217.

Finally, PO ignores Herrmann’s assigning policies to users. Pet., 27; Lee, ¶80. A POSITA would have added Herrmann’s gateway server and its access policy assignment functionality to Cidon’s management server. *Id.* In the combination, the gateway would have performed Herrmann’s “assign[ing] an access policy” retrieved “by **user**, by **group**, or by **computer**.” Herrmann, ¶¶67, 77; Pet., 26-27; Lee, ¶¶79-80.

2. Cidon’s policy met the “processing” limitation.

PO’s assertion that Cidon’s encryption policy did not govern the “processing of a file to be uploaded on a cloud” (POR, 3) overlooks Cidon’s disclosures that policies dictated file encryption before cloud upload. Cidon described encrypting specific files as per policy and its server managing these encrypted files’ cloud upload. Pet., 25; Cidon ¶¶224, 227, 57, 221. A POSITA would have understood that these *encrypted* files had been *processed* before they were uploaded based on encryption policies. Indeed, Dr. Black testified about this claim limitation that “process[ing]...could be almost anything.” Black Tr., 10:9-10. Cidon also disclosed another example where its server encrypted previously unencrypted files for cloud storage, which further shows that encryption and subsequent upload actions fall under the “processing” limitation. Pet., 25, 30; Cidon, ¶¶222, 227.

Further, PO’s citation to Dr. Lee is misleading. POR, 35. While acknowledging a “possible scenario” entails uploading unencrypted files to a secured folder, Dr. Lee explains Cidon’s system encrypted the files before uploading them to a cloud based on the policy. Lee Tr., 67:4-7; Cidon, ¶¶221, 227.

3. Cidon’s policy governed access management.

PO again argues for a “single policy” in the context of “access management” (POR, 35-36), which was addressed above. *See* §**Error! Reference source not found.**; *see also* Inst. Dec., 18-19. Moreover, as the Board correctly noted, Cidon

disclosed a *single policy* that “controls secure file access, encryption, storage, and management.” Inst. Dec., 25 (citing Cidon at ¶¶102, 108).

D. Claims 1/16: Cidon disclosed or rendered obvious “storing, by the gateway device” (claim 1) and “a storage module” for storing (claim 16) “the searchable encrypted file on the one or more cloud platforms based on the policy.”

PO’s same “single policy” argument regarding Cidon’s placement policies also fail as explained in Section **Error! Reference source not found.** POR, 39-41, 1-2. Further, Cidon disclosed a *single policy* based on which the searchable encrypted file is processed, encrypted, and stored.

Specifically, Cidon outlined a comprehensive policy framework that encompassed both placement and access management functions. Pet., 48-49. For example, Cidon’s placement policies dictated file locations within specific directories, and also defined access and sharing permissions, encryption protocols, and actions taken upon policy violations (e.g., alerting users and/or moving the file to reverse the violation). Cidon, ¶¶207-217. Cidon also described its system “encrypt[ed] files in consumer file repositories” and “IT departments [would] want[ed] different policies for access to *these secure files*.” *Id.*, ¶108. Thus, a POSITA would have understood that storing the searchable encrypted file on a particular cloud was based on Cidon’s comprehensive policy. Pet., 48-49; Lee, ¶110. And the Board acknowledged Cidon’s integrated approach, noting that Cidon’s system controlled secure file access, encryption, storage, and management through

a single policy. Inst. Dec., 25; *see also* §§III.C.2-III.C.3; Pet., 25, 29, 33-34, 46-49.

E. Claims 11/25: Cidon disclosed or rendered obvious storing a file “across two or more cloud platforms.

PO’s argument that “Cidon’s disclosure of ‘archiving and backup’ is with respect to ‘DNA extraction,’ not encrypted documents” (POR, 42) contradicts Cidon’s explanation that “the management server can be used not only for DNA extraction but also for other services such as *encryption,...archiving and backup to other storage services, and file synchronization between services.*” Cidon, ¶174.

Moreover, PO’s interpretation that storing “across” multiple platforms necessitates splitting a file into chunks for storage on different platforms (POR, 41) is neither required by claims 11/25, nor mandated by the ’678 patent’s specification. Specifically, the ’678 patent allows storage of *whole* files across cloud platforms, indicating that storing file chunks into different cloud platforms is optional. *See, e.g.,* ’678 Patent, 16:55-58 (describing “upload[ing] *each file*, whether in chunks or *not*,...onto one or *more* containers.”), 16:41-46 (“[P]artitioning the file into multiple parts/chunks is *not compulsory*....”), 1:47-51 (“stor[ing] data *across* multiple cloud platforms to ensure more security, *redundancy*....”). Thus, Cidon’s “archiving and backup to other storage services” and “file synchronization between services” mirror the file storing process “across multiple cloud platforms” in the ’678 patent. Cidon, ¶174.

F. Claim 14: Cidon disclosed or rendered obvious a policy that defines “one or more authorized locations to which the file may be stored.”

PO’s argument again relies on its erroneous “single policy” interpretation (POR at 43), dispatched in Section in **Error! Reference source not found..** Moreover, even under this interpretation, Cidon disclosed and/or rendered obvious the limitations relating to the “policy.” §§III.C.3-III.D.

Further, PO’s argument that “Cidon does not disclose that the authorized location(s) for storing the file is policy-based (POR, 42-43) was squarely addressed by Petitioner: “Cidon disclosed storing a modified file to a new location to prevent a user from directly accessing the location where the original file was stored” and a “POSITA would have found it *obvious* that the file locations would be part of Cidon’s security policy that could also define (and manage) such location information.” Pet., 64. PO has not rebutted this *obviousness* ground.

G. PO did not separately dispute Grounds 2 or 3.

By relying solely on its Ground 1 arguments (POR, 43), PO has waived any arguments specifically related to claims 6 and 15.

IV. GROUND 4: AURADKAR, CHIUEH, AND CHAMBERS RENDERED CLAIMS 1-3, 8-19, 21-27 OBVIOUS.

A. Claims 1/16: Auradkar in view of Chiueh rendered obvious “creating namespaces” or “configuring the namespaces.”

PO’s arguments in Ground 4 mirror those against the Cidon-Shikfa-Herrmann

combination. POR, 44. Namely, PO argues that:

- (1) creating identifiers does not create namespaces,
- (2) Chiueh's use of identifiers is not configuring namespaces,
- (3) Chiueh's use of identifiers is not part of encryption, and
- (4) a POSITA would not be motivated to add Chiueh's client-based encryption to Auradkar/Chambers.

Id. These arguments fail for the same reasons outlined for the Auradkar-Chiueh-Chambers combination, and the additional reasons below. *See* §§III.A-B.

1. Creating identifiers constituted creating namespaces.

As explained above, the '678 Patent does not describe how to create namespaces, and namespaces can include simple cases, such as naming a file (or chunk) with a specific identifier, like Auradkar's tags and Chiueh's document IDs. §III.A.1.

PO contends that Auradkar's and Chiueh's identifiers were members, not the namespace. POR, 44. This contention overlooks the broader functional aspect of namespaces. In fact, Dr. Black testifies that namespace is "a set of names. Names are typically values or data items, but that's a broad term that encompasses almost anything. A name can be almost anything." Black Tr., 40:22-41:3.

Auradkar disclosed creating tags for payloads (e.g., payload 1200, XML fragment 1902 (chunks)), such as **tag 1200** that included the filename of the payload (FName: fox.tx) and **XML tags 1900**, and encrypting them. Pet., 94-96; Auradkar,

¶¶125, 150, FIGS. 12, 19.

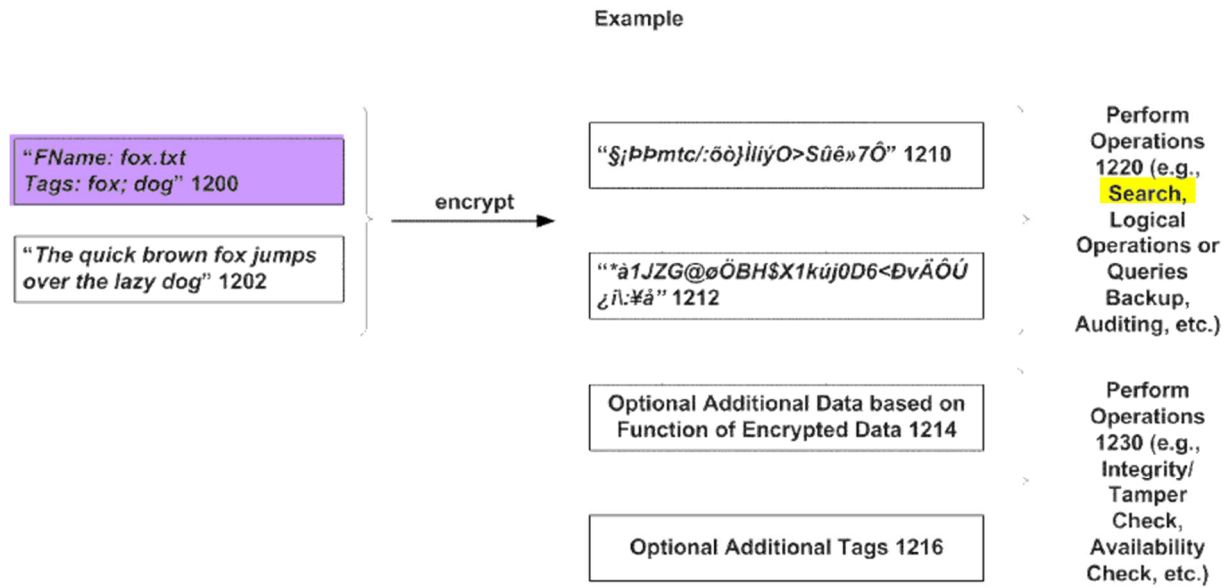


FIG. 12 (Annotated)

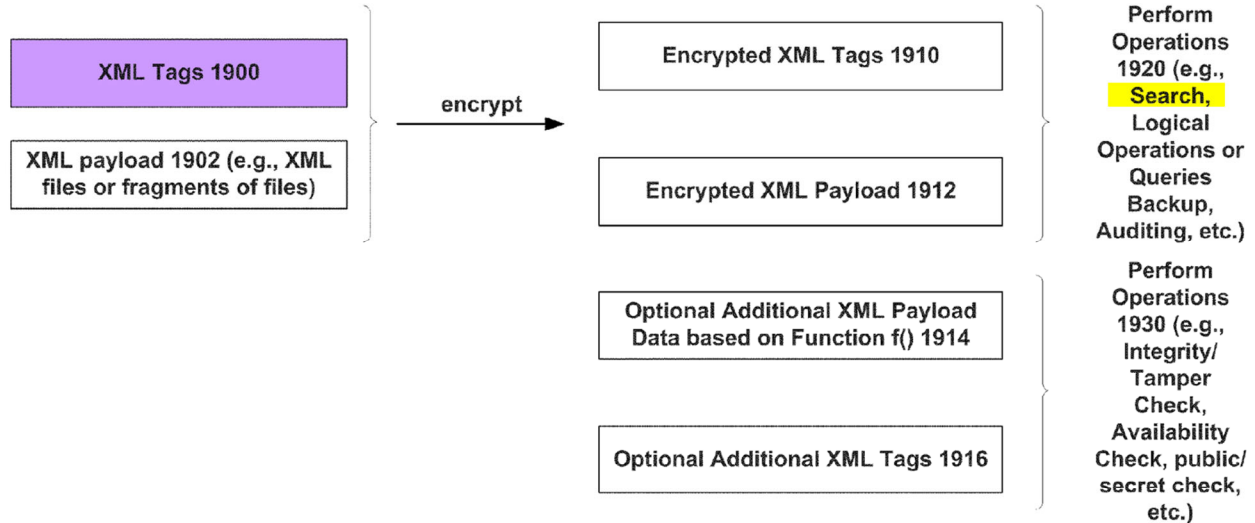


FIG. 19 (Annotated)

A POSITA would have found it obvious that these tags constituted

namespaces for the payloads (e.g., file 1202 or XML fragment), because they were a “set of names available for naming” these payloads. Pet., 96; Lee, ¶217. Thus, Auradkar’s creating these tags in association with the corresponding payloads constituted creating namespaces for these payloads.

Similarly, Chiueh divided a document into multiple pages, encrypted individual pages, and assigned a distinct document ID (a combination of a filename and a page offset in the document) to each page. Pet., 96-97; Chiueh, ¶20. These document IDs served as identifiers for the encrypted pages within the global search index. Pet., 96-97; Chiueh, ¶40. Chiueh’s document IDs constituted namespaces because they were a “set of names available for naming” encrypted pages. *Id.*

Even under PO’s interpretation of “namespace” requiring a context-specific name set, Auradkar’s tags and Chiueh’s document IDs satisfy the “namespaces” limitation, because they uniquely identify elements (individual encrypted XML segments or pages) within their respective contexts (among all encrypted XML segments or pages). This functionality of Auradkar’s tags and Chiueh’s document IDs as namespaces is affirmed by their use in facilitating search operations on encrypted payloads or pages, a process that relied on the functionality provided by namespaces—ensuring every encrypted payload or page can be identified uniquely by their identifiers. Pet., 94-97; Auradkar, ¶¶125, 150, FIGS. 12, 19; Chiueh, ¶¶20, 40; Lee Suppl., ¶14.

PO's argument that identifiers are merely members, not namespaces, overlooks the function of namespaces and their implementation in a system. While a filename *can* be considered a local name within a broader namespace, creating an identifier (based on a filename) and associating it with a particular file segment created a *namespace for that* file segment. Lee Suppl., ¶15. Notably, namespaces came into existence as these identifiers were being created and assigned to particular file segments, as these identifiers now became a set of unique names within the context of the encrypted file(s). *Id.*

PO again mischaracterizes Dr. Lee's testimony. POR, 46. Dr. Lee explained that the broader "documents" namespace *provides* a context within which the "foo" file is unique, which does not support PO's contention that filenames cannot be namespaces. Ex. 2004, 38:13-23; *see also id.*, 37:22-38:2, 39:6-40:1.

Further, PO's argument (POR at 24) that namespaces were not "created during the encryption process" because they were "created in advance" hinges on an impermissible interpretation requiring creating namespaces be part of encrypting content of the file and should be rejected. *See* §II.B. But, even under this interpretation, Auradkar disclosed creating tags (namespaces) during its encryption process. *Compare* '678 Patent, FIG. 3A *with* Auradkar, FIGS. 12, 19.

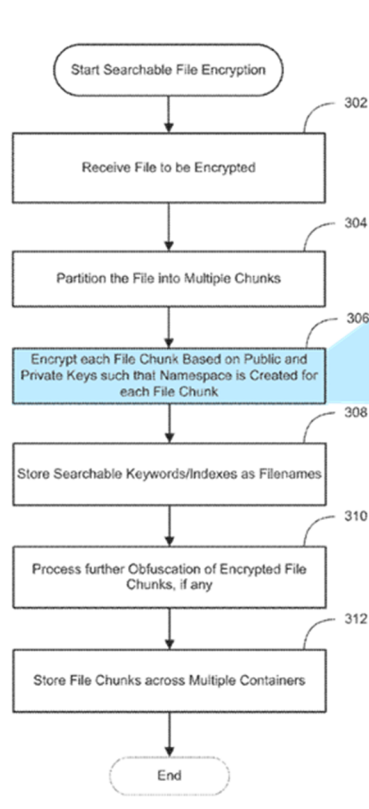


Fig. 3A

'678 Patent, FIG. 3A

(Annotated)

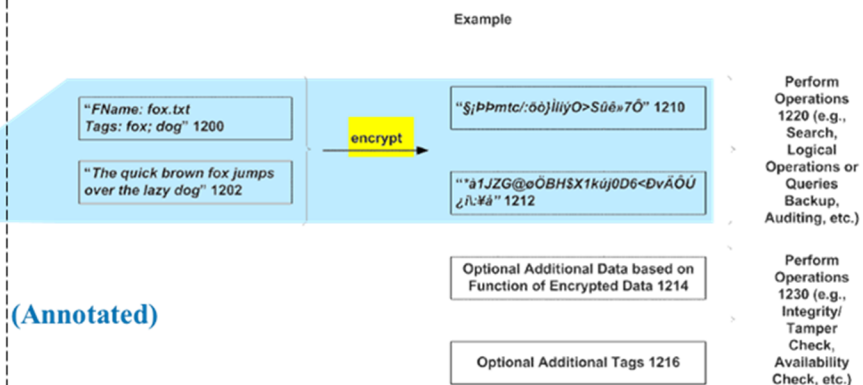
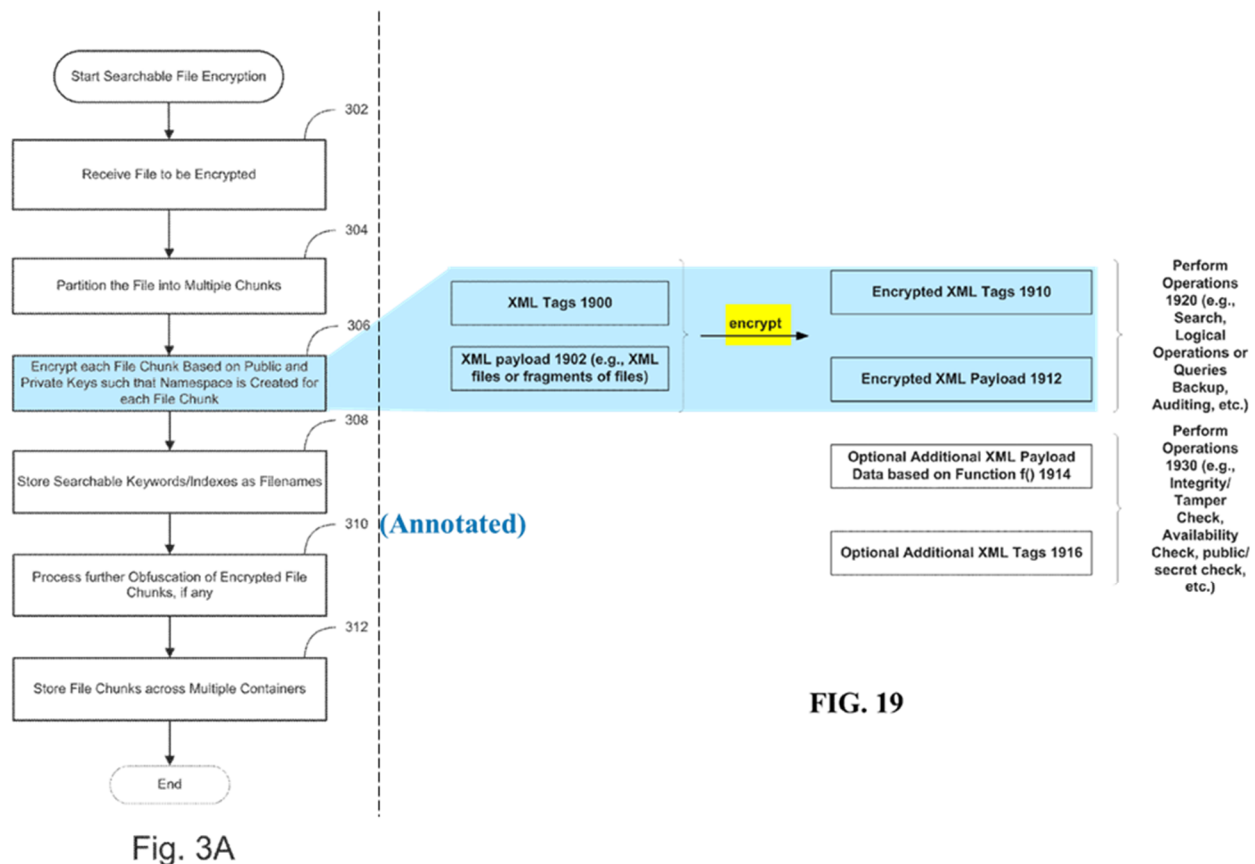


FIG. 12

Auradkar, FIG. 12.



'678 Patent, FIG. 3A

Auradkar, FIG. 19.

2. Chiueh's mapping of keywords to document identifiers constituted "configuring the namespaces."

PO first argues that Chiueh's mapping of keywords to document IDs does not "configur[e] the namespaces" because these identifiers are not namespaces. POR, 47-48. But, as explained above, Chiueh's document IDs constituted namespaces. *See* §IV.A.1.

PO next argues that Chiueh's document IDs were used within Chiueh's indexes but not configured. POR, 48. This argument mirrors an argument Petitioner has already rebutted above for the Cidon-Shikfa-Herrmann combination. *See*

§III.A.33. Specifically, as understood by a POSITA, configuring can be any of arrangement, use, or integration in a particular way to achieve a specific functionality—“content of the file is encrypted in a manner that makes it searchable.” *Id.*

Chiueh’s mapping of keywords to document IDs constituted “configuring the namespaces” because Chiueh created an index (a significant word set (SWS)) that mapped encrypted keywords to corresponding document ID(s) of the encrypted pages, so that the content of the encrypted pages could be searched using those keywords. Pet., 102-104; Chiueh, ¶¶21-23, FIG. 2.

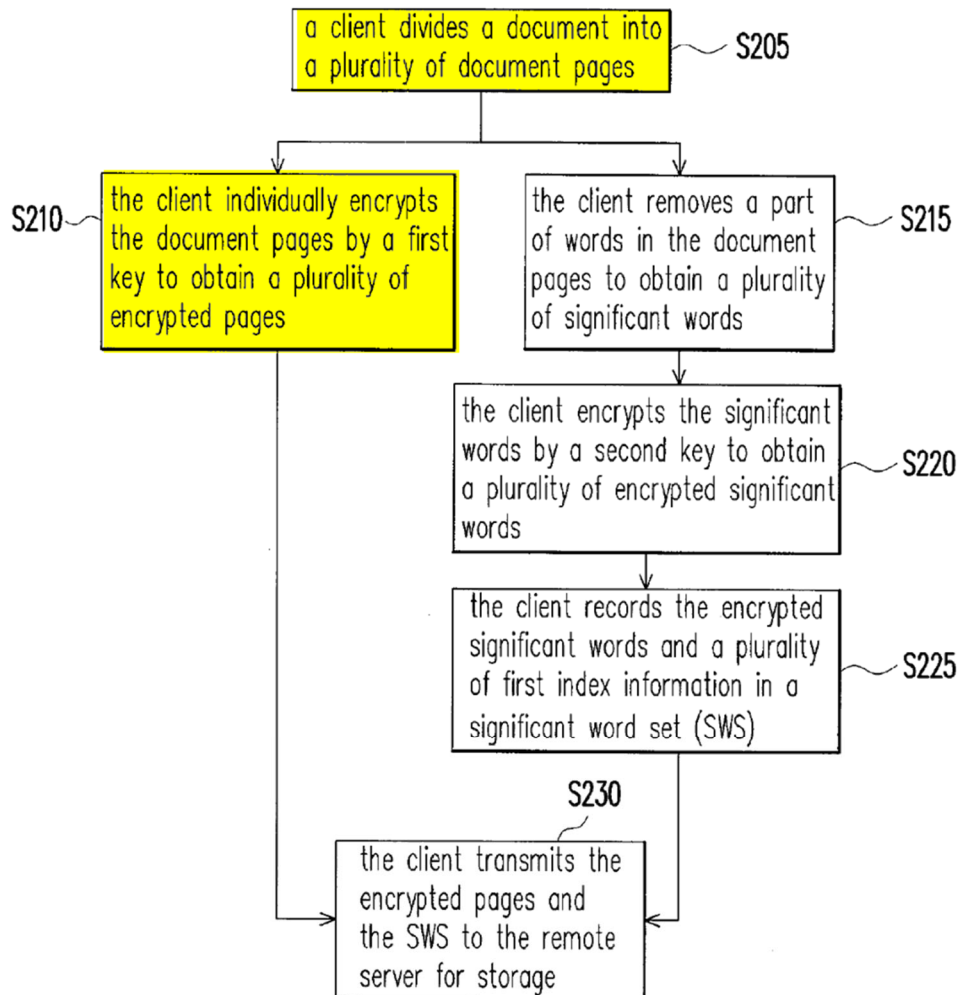


FIG. 2 (Annotated)

A POSITA would have understood that Chiueh's use of document IDs with the index pointing to encrypted pages *in a particular way* configured these IDs as part of a searchable encryption scheme to make the encrypted content searchable. Lee Suppl., ¶16; *see also* §III.A.3. This is consistent with '678 Appendix A, wherein hierarchical indices are generated by first hashing all cypher-texts and then generating a second hash for each cypher-text which indicates the key for a table in which many cypher-texts are aggregated. '678 Patent, Appendix A, Section V. The

table is stored at the cloud provider, and when the “cloud provider is queried for the table, [it] is then downloaded, loaded into memory, and then searched for the original cipher-text.” *Id.* Notably, in this technique the encrypted file is made searchable by using hierarchical indices stored in a table and subsequently used to locate the cypher-text of interest, akin to Chiueh’s creating an index that mapped encrypted keywords to corresponding document ID(s) of the encrypted pages, so that the content of the encrypted pages could be searched using those keywords. Pet., 102-104; Chiueh, ¶¶21-23, FIG. 2; Lee Suppl., ¶16.

Contrary to PO’s assertion (POR at 49-50),⁵ the claims do not require the “configuring” step be part of content encryption, but rather the namespaces be configured such that “content of the file is encrypted in a manner that makes it searchable,” which is exactly what Auradkar-Chiueh combination taught. Pet., 98-106; §II.B.

Further, as explained above, PO’s alleged “novel process” involving using the encrypted keywords as filenames cannot be imported into the independent claims

⁵ Again, Patent Owner mischaracterizes Dr. Lee. POR, 48. As explained in Section III.A.3, Dr. Lee used the terms “independent” and “orthogonal” to describe the flexibility in choosing encryption mechanisms for encrypting documents and indexes, not a separation of indexing and encryption. Lee Tr., 136:13-137:7.

that lack these limitations, because this “novel process” is one non-exclusive example. *See* §III.A.3.

3. A POSITA would have been motivated to combine Auradkar, Chambers, and Chiueh.

The Board has already rejected PO’s contention (POR at 50-52) of a lack of motivation to add Chiueh’s client-side encryption techniques into the Auradkar-Chambers combination. Inst. Dec., 44; *see also* §III.B.

Additionally, Chiueh’s searchable encryption mechanism is not limited by encryption location. Indeed, as noted by the Board, “the modification is to Auradkar, not Chiueh, *and*, a skilled artisan could weigh pros and cons and determine that the enhancement to Auradkar’s system would outweigh any perceived problems with using Chiueh’s document ID outside a client when Auradkar already uses similar XML tags to search XML fragments.” Inst. Dec., 44 (emphasis in origin).

Moreover, PO’s concerns (POR at 51)⁶ about the unreliability of a remote server in the encryption process, viewing it as untrusted, overlooks that in the Auradkar-Chambers combination, the gateway is controlled by the data-protecting entity, rendering PO’s alleged “peeked/leaked” risks moot.

⁶ Patent Owner’s statement about Dr. Lee’s testimony is again misleading. POR, 51. The quoted testimony was not about the physical location of encryption within the system. Lee Tr., 80:4-9, 82:20-24.

PO's teaching-away argument also fails. POR, 51. Specifically, Chiueh did not criticize, discredit, or otherwise discourage the use of its searchable encryption mechanism in a system with a gateway device *owned by the same entity* seeking to protect data like the one in the Auradkar-Chambers combination. *Meiresonne*, 849 F.3d at 1382.

B. Claims 1/16: Auradkar disclosed “cryptographic key information defined by the policy.”⁷

PO's contention (POR at 53-54) again hinges on interpreting “policy” as “single policy.” That has already been rejected by the Board and addressed in this Reply. Inst. Dec., 17-18; §§II.C., III.C.3, III.D-E.

But, even under PO's “single policy” interpretation, Auradkar taught a policy framework that is not limited to classifications of paragraphs within a document but extends to the policy for encryption mechanism, key, access, data storage. Auradkar, ¶¶108, 117, 95-96. As the Board correctly noted, “Auradkar describes details of the policy in other paragraphs does not negate this description of a policy.” Inst.

⁷ The POR and Dr. Black's supplementary declaration both assert “that “cryptographic key information” at least includes defining the encryption and/or decryption keys and encryption type.” POR, 53; Ex. 2003, ¶ 143. But during his deposition, Dr. Black confirmed that this definition is only an example based on one embodiment. Black Tr., 91:10-93:20.

Dec., 40.

C. Claims 1/16: Auradkar disclosed a policy for “processing of a file to be uploaded on a cloud.”

PO’s contention that Auradkar’s policy did not govern file processing before uploading to the cloud overlooks the broad scope of Auradkar’s policy. POR, 54-55. As the Board correctly noted, Auradkar’s enterprise access policy defined access rights, *encryption*, storage, and managing access. Inst. Dec., 40; *see also* Pet., 81-83, 88-93 (explaining that the Auradkar system *encrypted* files to be uploaded to a cloud according to the policy). Such encryption activities, performed pre-upload, were within the scope of file managing and processing governed by Auradkar’s enterprise access policy. Pet., 81-83; *see also* Black Tr., 10:9-10.

V. GROUND 5: AURADKAR AND INOUE RENDERED CLAIM 6 OBVIOUS.

PO’s argument that Inoue *alone* did not disclose or render obvious “wherein the step of configuring the namespaces comprises storing content of the file as filenames” mischaracterizes Petitioner’s proposed combination. POR, 55. Instead, Petitioner’s combination “incorporate[s] Inoue’s functionality of assigning a keyword [(file content)] extracted from file content (e.g., Auradkar’s keywords 1510) into the Auradkar-Chiueh-Chambers system to produce filenames that also included a keyword.” Pet., 137. PO has not rebutted *this* combination. *See* POR, 55-57.

Petitioner explained that Inoue’s functionality of *assigning keywords to*

filenames is added into the Auradkar-Chiueh-Chambers combination, which was already capable of extracting keywords from file content. Pet., 137. Specifically, Inoue’s contribution to the combined system is its technique for linking a keyword to a filename, irrespective of the keyword’s origin. Auradkar provided the teaching for extracting keywords from the content of a document, and Auradkar’s keywords are then used using Inoue’s functionality to create a searchable filename in the combined system. Pet., 135-137; Auradkar, ¶130.

VI. CONCLUSION

For these reasons, Petitioner requests the Board find the challenged claims unpatentable as obvious.

Dated: April 10, 2024

Respectfully submitted,

/Babak Tehranchi/

Lead Counsel

Thomas N. Millikan, Reg. No. 72,316

PERKINS COIE LLP

11452 El Camino Real, Suite 300
San Diego, California 92130-2080
858.720.5700 (phone)
858.720.5799 (fax)

Back-up Counsel

Babak Tehranchi (Reg. No. 55,937)
Andrew N. Klein (*pro hac vice*)
Wei Yuan (Reg. No. 71,772)

Attorneys for Petitioner

CERTIFICATE OF WORD COUNT UNDER 37 CFR §42.24(d)

Under 37 C.F.R. §42.24(d), the undersigned certifies that the word count for this **Petitioner's Reply To Patent Owner's Response** totals 5,543, excluding the parts exempted by 37 C.F.R. § 42.24(a). Accordingly, this paper is under the word count limit of 5,600 words.

The word count was made using the built-in word count function in the Microsoft® Word 365 software used to prepare this document.

Dated: April 10, 2024

PERKINS COIE LLP
11452 El Camino Real, Suite 300
San Diego, California 92130-2080
858.720.5700 (phone)
858.720.5799 (fax)

Respectfully submitted,

/Babak Tehranchi/

Lead Counsel

Thomas N. Millikan, Reg. No. 72,316

Back-up Counsel

Babak Tehranchi (Reg. No. 55,937)

Andrew N. Klein (*pro hac vice*)

Wei Yuan (Reg. No. 71,772)

Attorneys for Petitioner

CERTIFICATE OF SERVICE

I hereby certify that on April 10, 2024, I caused a true and correct copy of the foregoing **Petitioner's Reply To Patent Owner's Response** and supporting materials to be served electronic mail on the following attorneys of record for Patent Owner:

James M. Glass - jimglass@quinnemanuel.com
John T. McKee - johnmckee@quinnemanuel.com
Quincy Lu - quincylu@quinnemanuel.com
Andrew M. Holmes - drewholmes@quinnemanuel.com
Quinn Emanuel Urquhart & Sullivan LLP
51 Madison Ave, 22nd Floor
New York, New York 10010

Dated: April 10, 2024

Respectfully submitted,

PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101

/Anita Chou/
Anita Chou
Patent Paralegal