

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Netskope, Inc.

Petitioner,

v.

Fortinet, Inc.

Patent Owner.

Case No. IPR2023-00458

Patent No. 9,280,678

**DECLARATION OF DR. JOHN BLACK JR.
IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSE**

1. I have been retained on behalf of Fortinet, Inc. (“Patent Owner”) in connection with the above-captioned *inter partes* review (IPR). I have been retained to provide my opinions in support of Fortinet’s Patent Owner Preliminary Response. I am being compensated for my time at the rate of \$625 per hour. I have no interest in the outcome of this proceeding.

2. In preparing this Declaration, I have reviewed and am familiar with the Petition for IPR2023-00458, U.S. Patent No. 9,280,678 B2 (the “’678 patent”) and its file history, and all other materials cited and discussed in the Petition (including the declaration of Petitioner’s expert, Dr. Wenke Lee) and cited and discussed in this Declaration.

3. The statements made herein are based upon the cited documents as well as my own knowledge and opinion. This Declaration represents only the opinions I have formed to date. I may consider additional documents as they become available or other documents that are necessary to form my opinions. I reserve the right to revise, supplement, or amend my opinions based on new information and on my continuing analysis.

I. QUALIFICATIONS

4. My qualifications can be found in my Curriculum Vitae (*see* Ex. 2002), which includes my detailed employment background, professional experience, and list of technical publications and patents.

5. I am an Associate Professor of Computer Science at the University of Colorado, Boulder. I received a B.S. in Mathematics and Computer Science from the California State University at Hayward (now "California State University, East Bay") in 1988. I received an M.S. in Computer Science in 1997, and a Ph.D. in Computer Science in 2000, both from the University of California at Davis.

6. I have taught more than 60 classes in computer science, on subjects including data structures, algorithms, networking, operating systems, software engineering, security, cryptography, discrete mathematics, and quantum computing. I have authored or coauthored more than 20 publications, primarily on issues relating to computer security. I have been involved with computers for over 40 years in both commercial and academic capacities.

7. My earliest interest was in networks and security. My first memories in this regard were around 1975 when a group of friends and I learned about the telephone network and its security. A few years later, personal computers became available and I spent most of my free time studying, programming, and modifying them. I worked extensively with various networking products throughout the 1980s, and developed an interest in cryptography soon thereafter. Although my undergraduate institution had no courses in cryptography or security in the 1980s, I decided to pursue self-study at the time, and opted to double major in Computer Science and Mathematics because cryptography is a blend of these two subject areas.

8. After earning my B.S. degree in 1988, I worked for six years at Ingres Corp as a software developer, writing and reviewing code written in C. My work primarily was directed at transaction logging, data type support, and security.

9. In 1995, I began my Ph.D. at UC Davis under cryptographer Phillip Rogaway. My area of focus was cryptography and security and my research involved encryption, authentication, hash functions, and network security.

10. After graduation I took a position as an Assistant Professor at the University of Nevada at Reno. In the Fall of 2001, I taught the networking class there, which included coverage of Ethernet, interior gateway protocols, exterior gateway protocols, ARP, DHCP/BOOTP, IP, UDP, TCP, HTTP, SMTP and other protocols. In 2001, a graduate student and I looked at the security of ARP and invented a new protocol "AuthARP" to add security to the protocol.

11. In 2002, I moved to the University of Colorado at Boulder where I am currently employed. In the Fall of 2002, I co-designed and co-taught a new course called "Foundations of Computer and Network Security," which included descriptions of security issues around both wired and wireless security challenges, mostly for public-facing network services including the world-wide web. I have taught this class seven more times since then, including modern topics such as wireless networking, the Internet of Things, and so forth.

12. In my career at the University of Colorado, I have published several more papers in the area of cryptography and network security. I have taught more than 30 courses in network security and cryptography, and have graduated several PhD students in these areas.

13. I also have worked for a consulting company at times, writing software on contract basis. Although most projects are covered by NDAs, many involved networks and/or aspects of computer security.

14. In 2011, I began technical consulting for a local company called Cardinal Peak, which focuses primarily on video encoding and delivery systems. My work for Cardinal Peak has largely been directed to video encoding, transcoding, compression, encryption, and DRM, but also has included networking projects and embedded device work. For example, I designed the security system for the Pro1 smart thermostat, implemented the DRM for the Yonder Music App, worked on 802.1X code for smart dog collars, and helped design the cryptography used in Fitbit devices for wireless transfer of a Fitbit watch to a phone or laptop.

15. In 2016, I took a two-and-a-half year leave of absence from the University of Colorado to start a company named "SecureSet" in Denver, Colorado. The objective of SecureSet is to take reasonably proficient technical people and turn them into computer and network security specialists via five months of intensive training. SecureSet was sold to WeWork in 2019 and continues to offer computer

security classes today. In 2018 I returned to my position at the University where I remain employed to the present day.

II. LEGAL UNDERSTANDING

A. The Person of Ordinary Skill in the Art

16. I understand that a person of ordinary skill in the relevant art at the time of the invention (also referred to herein as “POSITA”) is presumed to be aware of all pertinent art, thinks along conventional wisdom in the art, and is a person of ordinary creativity—not an automaton.

17. I have been asked to consider the level of ordinary skill in the field that someone would have had at the time the claimed invention was made. In deciding the level of ordinary skill, I considered the following:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the field; and
- the sophistication of the technology.

18. A person of ordinary skill in the art relevant to the ’678 patent at the time of the invention would have had a Bachelor of Science degree in electrical engineering and/or computer science, and two years of work or research experience in the fields of network and data security, or a Master’s degree in electrical

engineering and/or computer science and one year of work or research experience in related fields.

19. I have reviewed the declaration of Dr. Lee, including his opinions regarding the Person of Ordinary Skill in the Art. My description of the level of ordinary skill in the art is essentially the same as that of the Dr. Lee. The opinions set forth in this Declaration would be the same under either my or Dr. Lee's proposal.

20. I am well-qualified to determine the level of ordinary skill in the art and am personally familiar with the technology of the '678 patent. I was a person of at least ordinary skill in the art at the time of the priority date of the '678 patent. Regardless if I do not explicitly state that my statements below are based on this timeframe, all of my statements are to be understood as a POSITA would have understood something as of the priority date of the '678 patent.

B. Legal Principles

21. I am not a lawyer and will not provide any legal opinions. Though I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

1. Obviousness

22. I understand that to obtain a patent, a claimed invention must have, as of the priority date, been nonobvious in view of prior art in the field. I understand

that an invention is obvious when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art.

23. I understand that to prove that prior art, or a combination of prior art, renders a patent obvious, it is necessary to: (1) identify the particular references that singly, or in combination, make the patent obvious; (2) specifically identify which elements of the patent claim appear in each of the asserted references; and (3) explain how the prior art references could have been combined to create the inventions claimed in the asserted claim.

24. I understand that a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art, and that obviousness cannot be based on the hindsight combination of components selectively culled from the prior art to fit the parameters of the patented invention.

25. I also understand that a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant. Even if a reference is not found to teach away, I understand its statements regarding preferences are relevant to a

finding regarding whether a skilled artisan would be motivated to combine that reference with another reference.

2. *My Understanding of Claim Construction Law*

26. I have been informed that patent claims are construed from the viewpoint of a person of a POSITA and that patent claims generally should be understood consistent with their ordinary and customary meaning at the time of the invention. A review of the patent claim language, the patent specification, and its prosecution history are also necessary to determine the proper meaning and scope of the term at issue.

27. I have further been informed that in the specification and prosecution history the patentee may define a claim term in a way that differs from the ordinary and customary meaning. I understand that during prosecution of the patent before the U.S. Patent and Trademark Office, the Applicant may make representations or provide definitions of terms that may affect the scope of the patent claims. In particular, the Applicant may, during the course of prosecution, limit the scope of the claims to overcome prior art and/or disavow claim coverage by making clear and unambiguous statements to that effect.

28. I have been informed that a POSITA may, among other things, consider dictionaries, publications, other patents, and treatises (*i.e.*, “extrinsic evidence”). I understand that extrinsic evidence may generally not be relied on if it contradicts the

meaning of claim language provided by the intrinsic evidence, such as express definitions given for terms in the specification.

III. OVERVIEW OF THE '678 PATENT

A. The '678 Patent Specification

29. The '678 patent is entitled “Secure Cloud Storage Distribution and Aggregation.” The patent provides a vendor independent secure cloud storage solution that introduces new systems and methods for “implementing a policy based framework for encrypting, storing, accessing, querying and managing data across one or more cloud platforms.” Ex. 1001, 3:23-28. Examples of cloud platforms include Dropbox, Google Drive, Amazon Web Services, etc. *Id.*, 6:9-14.

30. In some embodiments, the '678 patent provides a cloud storage distribution and aggregation service via a cloud storage gateway device situated between third-party cloud storage platforms and users. *Id.*, Abstract. Among other attributes, the service may provide an API that supports both file storage and search requests across stored files, along with the ability to remit content from stored files according to the search results. Moreover, the service may assign policies that can be assigned to users that determine access rights, storage attributes, encryption type, etc. *Id.* And when a file storage request is received, the service may create encrypted data suitable for that user's policy, and then distribute the associated ciphertext

among the third-party cloud storage providers based on storage requirements, again as defined by the user's policy. *Id.*, 2:10-30.

31. In the example shown below in Figure 2, the '678 patent provides a system that operates as an intermediary "Gateway" [204], highlighted below, which enables "interactions between enterprise users [202a, 202b, 202c] and cloud service providers [206a, 206b, 206c] for storage, retrieval, and searching of data and content stored by the providers." *Id.*, 8:27-9:4.

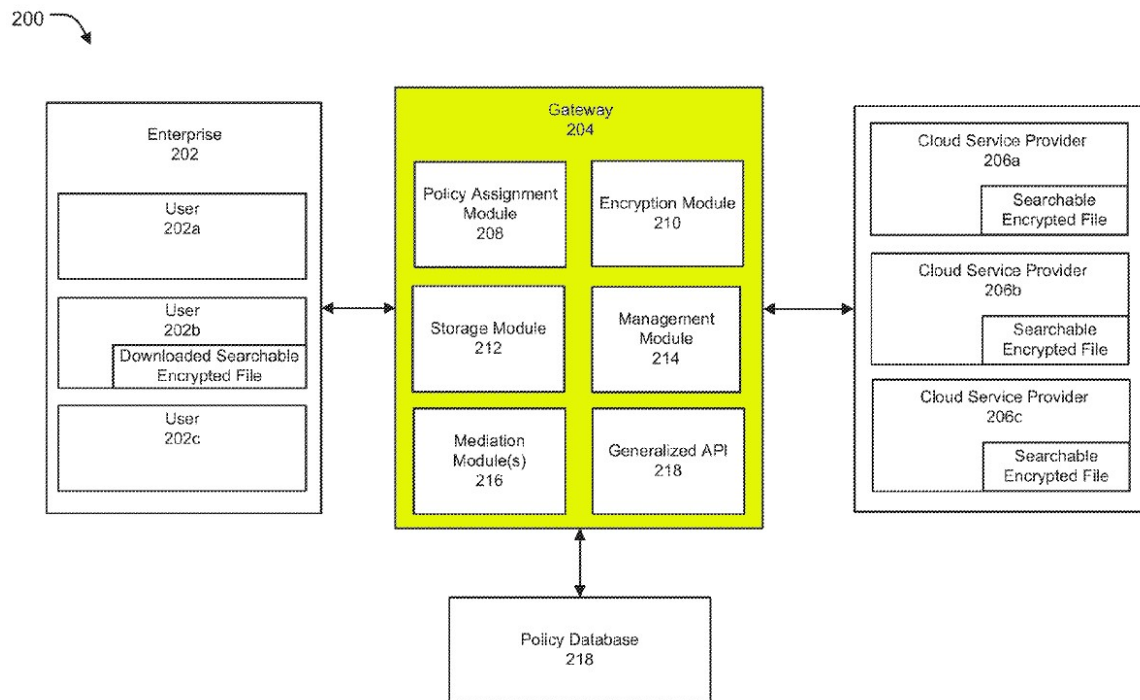


Fig. 2

32. In this example, users within an Enterprise 202 interact with Gateway 204 in order to access cloud storage via cloud storage providers 206. The policy assignment module 208 selects and assigns policies from the policy database 218 to

one or more enterprise users 202. *Id.*, 9:10-25. And the encryption module 210 encrypts files that are stored across one or more cloud platforms based on the given user policy. *Id.*, 9:53-56.

33. While typical prior art cloud storage systems allowed for only “rigid and non-flexible” interactions between enterprises and individual cloud service providers, the ’678 patent’s Gateway system gives enterprises the ability to more easily “store data across multiple cloud platforms to ensure more security, redundancy, and reduction in potential threat of data compromise,” as well as the ability to implement global file storage policies that “allow storage of data across different service providers, allow different cloud storage access rights across users and computing devices, [and] allow searching of downloaded encrypted data across cloud service vendors.” *Id.*, 1:38-2:30. As the ’678 patent explains, the Gateway may assign users a policy that “not only defines the manner in which the users can access and process content stored on the cloud, but can also configure the mode in which the data is encrypted, stored, searched, and accessed to ensure secure and vendor independent cloud management.” *Id.*, 3:28-67.

34. The ’678 patent also recognizes that storing files on cloud platforms in an “unencrypted format” may expose them to “network attack[s] that may lead to the [files] being compromised.” *Id.*, 1:52-54. For this reason, the Gateway can “encrypt one or more files to be uploaded/stored” using “cryptographic key

information” defined by the assigned policy. *Id.*, 4:1-12. But because the ’678 patent recognizes that conventional encryption techniques also “make[] the files ... unsearchable and hence unfriendly for user access” (*id.*, 1:54-57), the Gateway is able to produce a “searchable encrypted file” via a process that involves “dividing the file into [] chunks; creating namespaces for one or more of the [] chunks; and configuring the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.” *Id.* 19:62-20:3; *see also* Fig. 3A.

35. Importantly, applying the searchable encryption process at the Gateway system provides major advantages over traditional prior art systems. Some prior art systems relied on the individual client devices to encrypt files before storing them on a cloud platform, but this approach can make it harder for enterprises to implement global policies that allow other authorized client devices and users in the enterprise to search for and access the encrypted files. In comparison, the ’678 patent’s Gateway system provides enterprises with these capabilities. *See, e.g., id.*, 17:21-18:37. And still other prior art systems relied on the cloud service provider to perform file encryption and enforce access control policies, but this created the risk that the files could be “exposed to attack within the cloud, insider jobs and subpoena—all without the knowledge or consent of the data owner.” *Id.*, 1:59-62. In comparison, the ’678 patent’s Gateway may implement the patent’s searchable

encryption process “independent of the vendor/service provider of the cloud platforms.” *Id.*, 10:1-6.

36. This combination of features in the ’678 patent provides a more secure, flexible, and user-friendly cloud storage solution than what existed in the prior art.

37. Another advantage the ’678 patent provides, in some embodiments, is the ability for enterprises and/or their users to specify data storage diversity requirements via their policies (e.g., enterprises/users may specify a variety of third-party cloud storage providers in order to prevent vendor “lock in”), and to switch to other service providers, as desired, by changing policy. This feature not only provides flexibility and robustness, but also means that a user’s data is distributed to a diverse set of storage entities, thereby increasing security. *Id.*, 1:38-51.

38. Moreover, another advantage the ’678 patent provides, in some embodiments, is simultaneous use of searchable encryption so that large datasets can be searched by a user without the need to retrieve the full file, decrypt it locally, and then search. In some cases, encrypted data stored via a third party cloud provider involves encryption keys controlled by the cloud provider, meaning that the provider could potentially decrypt and thereby obtain the user’s data without the user’s consent or knowledge. This means that insider attacks, outside breach, subpoenas and other avenues of attack would be possible. By taking the keys out of the control of the cloud provider, these risks are reduced. *Id.*, 1:52-63.

39. In addition, another advantage the '678 patent provides, in some embodiments, is the provision of a single API that provides a simple uniform abstraction, instead of requiring developers to learn each specific vendor API for each of the underlying cloud providers. *Id.*, 1:63-2:5.

40. Still other advantages are described and/or made evident elsewhere in the '678 patent's specification.

B. The '678 Patent Claims

41. I understand Petitioner challenges independent claims 1 and 16 and dependent claims 2-3, 6, 8-15, 17, and 21-27 of the '678 patent.

42. By way of example, Claim 1 recites:

1. A method comprising:

assigning to one or more users, by a gateway device, a policy for managing access to and processing a file to be stored on one or more cloud platforms, wherein the policy defines access rights of the one or more users;

encrypting, by the gateway device, using cryptographic key information defined by the policy, content of the file to produce a searchable encrypted file by:

dividing the file into a plurality of chunks;

creating namespaces for one or more of the plurality of chunks; and

configuring the namespaces of the one or more chunks Such that content of the file is encrypted in a manner that makes it searchable;

storing, by the gateway device, the searchable encrypted file on the one or more cloud platforms based on the policy; and

managing access to the searchable encrypted file by the one or more users based on the policy.

43. Claim 1 of the '678 patent captures many of the central elements of the invention that I described above. Among other things, a gateway device assigns a policy for managing access to a file stored on one or more cloud platforms, the file is encrypted using a searchable encryption algorithm and stored in chunks on the one or more cloud platforms based on the policy, and access to the file is thereafter managed by the policy.

IV. OVERVIEW OF CERTAIN ART

44. The petition cites to a number of references, but the only references it relies on in challenging the independent claims are Cidon, Shikfa, Herrmann, Auradkar, Chiueh, and Chambers. The petition's first ground asserts that the combination of Cidon, Shikfa, and Herrmann renders obvious the independent claims (as well as some of the dependent claims). The petition's fourth ground asserts that the combination of Auradkar, Chiueh, and Chambers also renders obvious the independent claims (as well as some of the dependent claims). (Grounds 2, 3, and 5 of the petition address only dependent claims). Below, I briefly summarize Cidon, Shikfa, Herrmann, Auradkar, Chiueh, and Chambers.

A. Cidon (Ex. 1004)

45. Cidon is primarily directed to systems and methods for encrypting files stored on cloud-based storage services. Cidon, ¶10. Cidon depicts its basic method for encrypting a file in Figure 15, shown below. *See also id.*, Abstract, ¶10.

However, importantly, a POSITA would have understood that Cidon never discloses that any of its file encryption methods encrypt the content of a file in a manner that makes the content searchable.

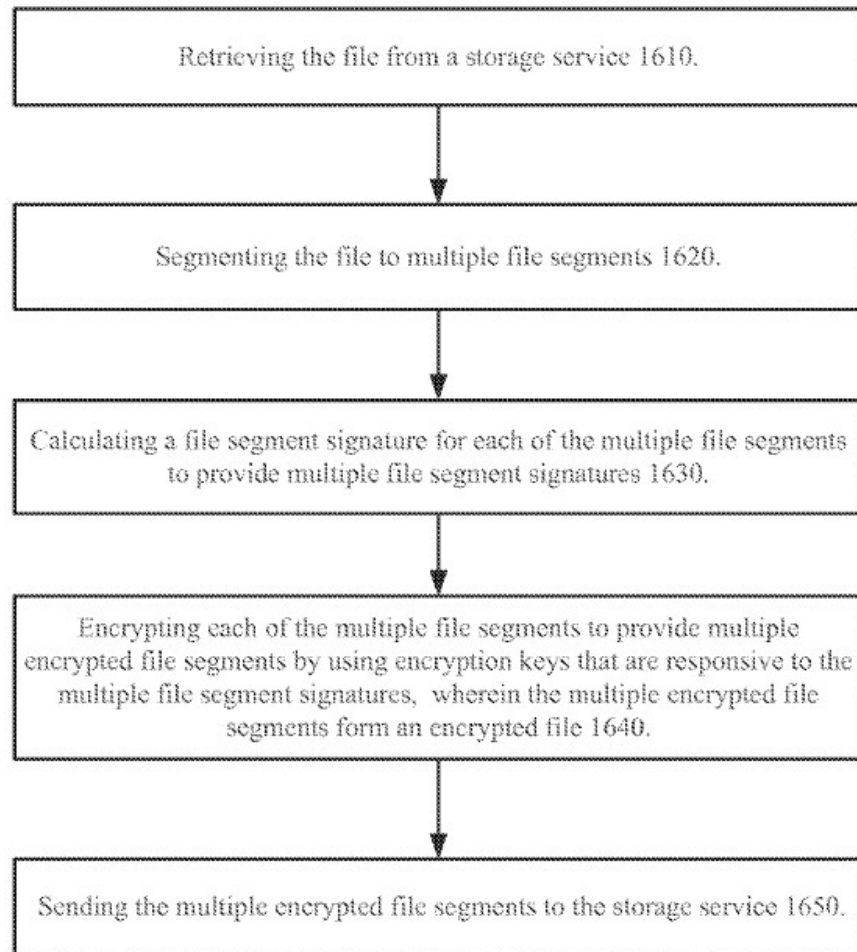


FIG. 15

46. Cidon teaches that its file encryption methods are implemented by a “management server,” which Cidon clearly explains is a “complete software system

which is responsible for encrypting files in the cloud and enforcing secure access to these cloud files by providing the right decryption keys to the right users.” *Id.*, ¶102, Fig. 2. The management server includes an “IT Policy Enforcement Module” that enforces user “access policies” controlling the ability for users to access secure files. *Id.*, ¶108. But, importantly, a POSITA would have understood that Cidon never discloses that these user “access policies” also define cryptographic key information or otherwise control the encryption and storage of files on cloud storage systems.

B. Shikfa (Ex. 1006)

47. Shikfa is primarily directed to a “system and method for enabling searchable encryption of encrypted documents stored by a client on one or more storage providers.” Shikfa, Abstract. Shikfa’s system includes a “broker server,” which “transfer[s] the encrypted documents between the client and the one or more storage providers[,] maintain[s] information indicating where the encrypted documents are transferred[,] [and] stores information for at least one encrypted index for the encrypted documents.” *Id.* But, importantly, Shikfa clearly teaches it is the client, not the broker server, that “encrypts the one or more documents” and “generate[s] [the] one or more encrypted indexes.” *Id.*, ¶29. Shikfa teaches that performing these functions at the client “ensures that the broker server 12 cannot access and/or discover the content of the client's data because the broker server 12 does not know the encryption used on the encrypted documents.” *Id.*, ¶48. Shikfa

explains that this aspect of Shikfa’s system is important for “maintaining the confidentiality of data external to the client.” *Id.*; *see also* ¶50.

48. Notably, Shikfa discloses that the client may encrypt documents and generate encrypted indexes using any “encryption mechanism known in the art.” *Id.*, ¶29. But, importantly, a POSITA would have understood that Shikfa never discloses performing an encryption process that divides the documents into chunks and creates and configures namespaces for one or more of the chunks.

C. Herrmann (Ex. 1005)

49. Herrmann describes technologies for “anti-virus cooperative enforcement.” Herrmann, Abstract, ¶¶48-50. For example, Herrmann explains that “[b]efore ... a client computer[] is permitted to join a network or access protected resources, a check is made to evaluate the antivirus engine and virus definitions that are installed and in use on [the client computer].” *Id.*, ¶50.

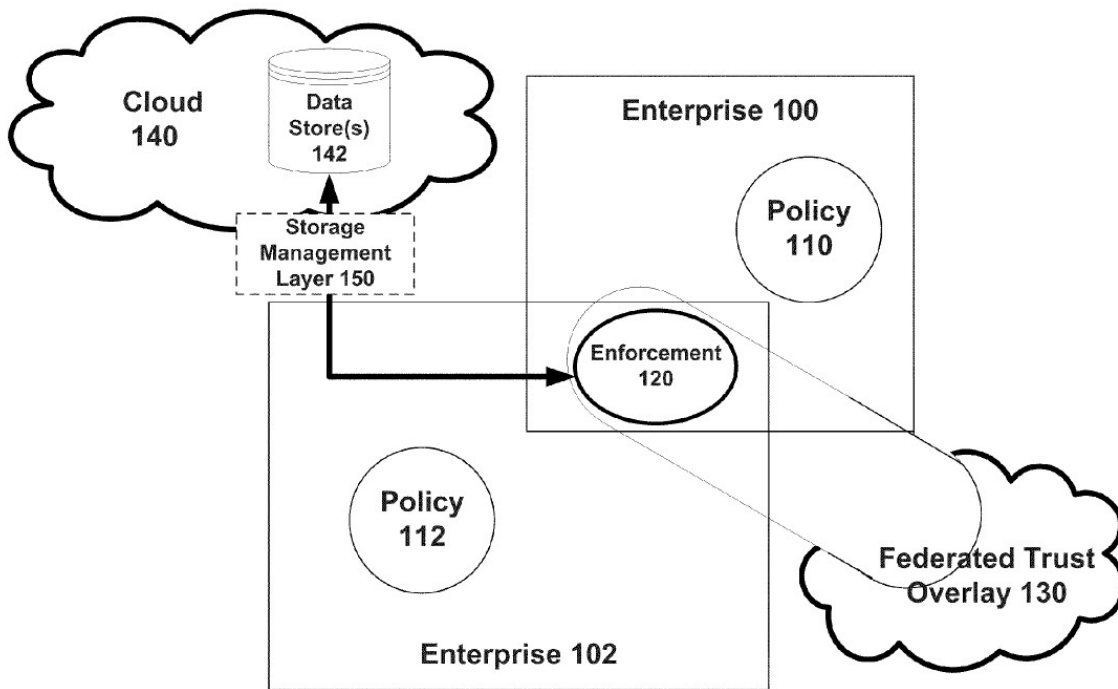
50. Herrmann further explains that “when a client computer requests a VPN connection to a gateway server, the system ... determines whether or not a client computer is using an approved anti-virus application.” *Id.*, ¶50. Herrmann teaches that the system makes this determination through a series of interactions between the client computer and what Herrmann describes as a separate “integrity server.” *Id.*, ¶29; *see also* Figs. 3-4. Only “[a]fter the integrity server 370 has evaluated compliance with anti-virus policies or rules, it notifies the gateway server about

whether to permit or restrict access by this particular client device,” and “[t]he gateway server may then decide how much access to permit by this particular client device (i.e., the gateway server 350 assigns an access policy to the connection/session between the gateway server 350 and the client computer 310) based upon the notification.” *Id.*, ¶77.

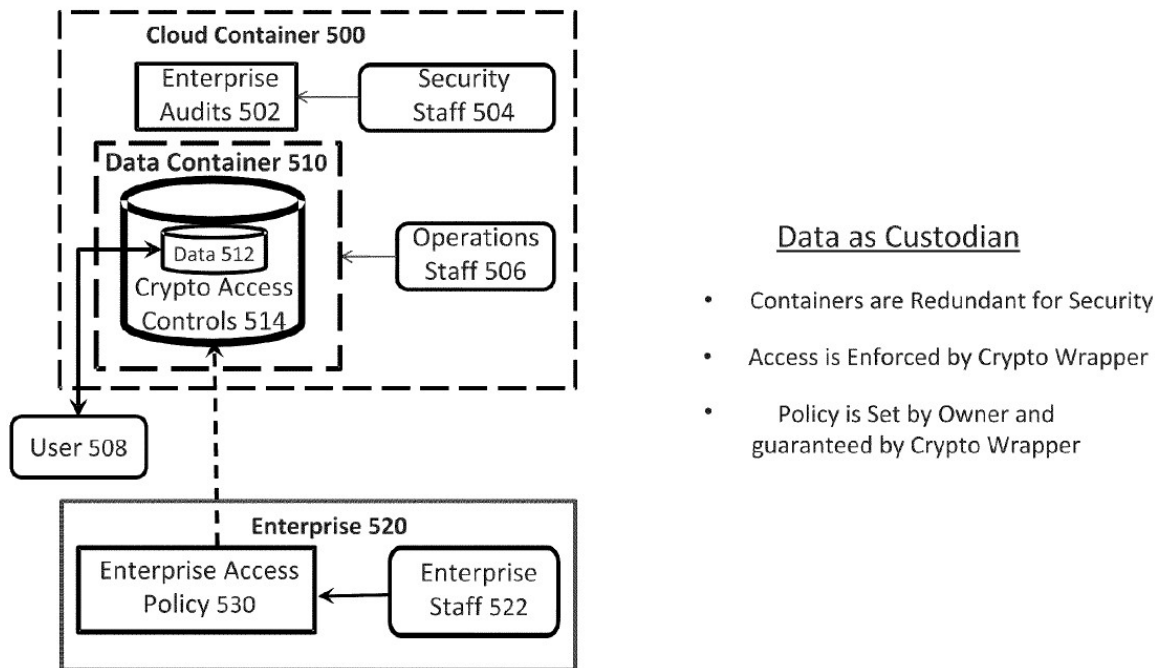
51. Importantly, a POSITA would have understood that Herrmann never discloses using its anti-virus cooperative enforcement system in connection with encrypting, storing, or controlling access to files stored on the cloud. In fact, Herrmann does not reference cloud storage at all, and it appears to be working in a completely different setting than the ’678 patent.

D. Auradkar (Ex. 1009)

52. Auradkar aims to provide a comprehensive “trustworthy platform” in which “data services, including mathematical transformation techniques, such as searchable encryption, deassembling/reassembling or distribution techniques, for data, are provided in a way that distributes trust across multiple entities ... and decouples data protection requirements ... from the containers that hold the data (e.g., file systems, databases, etc.) enabling the data to act as its own custodian.” Auradkar, ¶¶9-10. According to Auradkar, Figure 1 below depicts “a general environment for providing one or more embodiments of secure, private and selectively accessible network data services as described herein.” *Id.*, ¶110.

**FIG. 1**

53. Auradkar teaches that Figure 5 below illustrates more specific “aspects of data acting as its own custodian,” wherein “an enterprise 520 has enterprise staff 522 that can are subject to enterprise access policy 530 ... [that] can affect how data 512 stored in a data container 510 of a cloud container 500 can be accessed, manipulated, retrieved, searched, etc.” *Id.*, ¶¶116-117. But, importantly, a POSITA would have understood Auradkar never discloses that these “access polic[ies]” governing “users seek[ing] access to data” also define cryptographic key information or otherwise control the encryption and storage of this data on cloud storage systems.

**FIG. 5****E. Chiueh (Ex. 1011)**

54. Chiueh is primarily directed to a “document processing method and ... system” that is intended to “improve information security of remote storage documents, and facilitate a remote server to deal with various data processing requirements,” including keyword searching. Chiueh, ¶7. Chiueh’s system includes a “client [] connected to [a] remote server through a communication network.” *Id.*, ¶9, Fig. 1. Chiueh clearly teaches that before storing a document, the client performs a series of steps to create “encrypted pages” and a “significant word set (SWS),” which “the client transmits ... to [the] remote server for storage.” *Id.*, ¶¶8-9, Fig. 2.

55. Importantly, Chiueh (like Shikfa) clearly teaches that its document processing method is performed by the client, and that Chiueh's method should not be performed by the remote server, so that "the remote server does not have the keys [and it can] not decrypt the document pages and the significant word set." *Id.*, ¶10. Chiueh teaches that this is important because "the remote server is probably not reliable," and if "the remote server ha[d] the decryption capability, the client could not prevent an unfaithful query processing of the remote server," and "the document stored in the remote server could be peeked/leaked." *Id.*, ¶5.

F. Chambers (Ex. 1010)

56. Chambers is primarily directed to "[t]echniques for managing access control policies" that control access to computer networks. Chambers, Abstract. More specifically, Chambers describes "[t]echniques for automatically assigning access control policies (ACPs) based on device types of network client devices (NCDs)." *Id.*, ¶21. Chambers explains that "[w]hen a network device first connects to the network, it is examined by the system, identified by type, and assigned an access policy according to the specified rules for that device type." *Id.* This network access policy specifies network parameters, such as "bandwidth limits and traffic shaping rules, VLAN assignment, firewall rules, whether a captive portal should be applied to that device, etc." *Id.*, ¶¶32-40.

57. Chambers teaches that these network access policies are assigned and enforced by “network access devices (NADs) ... managed by a management server.” *Id.*, ¶24; Fig. 1. The NADs “may operate as a gateway device, an access point (AP), a network switch, or a combination thereof.” *Id.* Chambers further explains that these network access policies are initially “downloaded from management server 101 to [the] network access device” under the management server’s control, and then “[w]hen a client device ... is associated with [the] network access device 102, [the NAD’s] access control module 116 controls [network] access of [the] client device 108 by enforcing [the] ACPs.” *Id.*, ¶28, Fig. 6.

58. Importantly, a POSITA would have understood that Chambers (like Herrmann) never discloses using its network access control policy management techniques in connection with encrypting, storing, or controlling access to files on cloud storage systems. In fact Chambers, like Herrmann, does not reference cloud storage at all.

V. CLAIM CONSTRUCTION

59. In my opinion, no claim terms presently require construction. I reserve the right to proffer a construction for a claim term at a later point if I believe it pertinent to any particular dispute.

60. I have interpreted all claim terms as they would have been understood by a POSITA at the time of the priority date of the ’678 patent.

VI. THE PETITION FAILS TO SHOW THAT CIDON, SHIKFA, AND HERRMANN RENDER CLAIMS 1-3, 8-14, AND 16-27 OBVIOUS (GROUND 1)

A. The Petition Fails to Show the References Render Obvious the “Policy for Managing Access to and Processing a File”

61. Independent claim 1 recites “a policy for managing access to and processing a file to be stored on one or more cloud platforms.” Ex. 1001, claim 1[a][i]. Similarly, independent claim 16 recites a “policy [that] defines and manages access to and processing of a file to be uploaded on a cloud.” *Id.*, claim 16[c][i][A].

In addition, both claims further require:

- (1) that “the policy defines access rights of the [one or more] user[s]” (*id.*, claims 1[a][ii], 16[c][i][B]);
- (2) encrypting content of the file “using cryptographic key information defined by the policy” (*id.*, claims 1[b], 16[c][ii][A]);
- (3) storing “the searchable encrypted file on the one or more cloud platforms based on the policy” (*id.*, claims 1[c], 16[c][iii]); and
- (4) managing “access to the searchable encrypted file by the [one or more] user[s] based on the policy” (*id.*, claims 1[d], 16[c][iv]).

62. In my opinion, Petitioner does not show that the asserted references disclose or render obvious a single “policy” that meets all of the claim requirements discussed above. Instead, Petitioner points to several very different policies in Cidon, incorrectly treating them as if they were the same policy. For example, in asserting that Cidon discloses a policy that “defines access rights of the one or more users,” Petitioner points only to Cidon’s disclosure of user “access policies” that

control user access to secure files. *See* Pet. 29 (discussing Cidon, ¶¶102, 108, 112, 115); Pet. 53 (citing back). However, in asserting that Cidon also discloses “storing the searchable encrypted file ... based on the policy,” Petitioner instead points only to Cidon’s separate disclosure of file “placement policies” that control placement of files based on their relationship with other files. *See* Pet. 48-49 (discussing Cidon, ¶¶208-209, 214-215); Pet. 55 (citing back). And this pattern of mixing and matching of Cidon’s dissimilar policies occurs throughout the first ground of the petition. *See* Pet. 25, 29, 33-34, 48-49, 53-36.

63. A POSITA would have understood that the user “access policies” and the file “placement policies” in Cidon are totally different policies. First, user “access policies” are “define[d]” for “users” and “groups” of “[u]sers in a company.” Cidon, ¶108. In contrast, file “placement policies” are “defined on documents” or other files. *Id.*, ¶¶206-207. Second, user “access policies” are used to control user “access to [] secure files” in “file repositories” *Id.*, ¶108. In contrast, file “placement policies” are used to control storage operations on files, such as the “[p]lacement [of files] in specific directories or shares.” *Id.*, ¶¶206-209. Third, user “access policies” are defined by “administrators” in order to control users’ access to secure files. *Id.*, ¶108. In contrast, “users [can] change the [file placement] policy if needed.” *Id.*, ¶¶213-217. In addition, a POSITA would understand that Cidon discusses the user

“access policies” and file “placement policies” in completely different portions of the reference, and it never discloses that they are related in any way.

64. Importantly, Petitioner never shows or even alleges that a POSITA would have considered Cidon’s dissimilar user “access policies” and file “placement policies” to be the same single “policy” recited by the claims. In fact, for the reasons discussed above, a POSITA would have understood that Cidon’s user “access policies” and file “placement policies” are not the same policy.

65. In addition, Petitioner never shows or even alleges that it would have been obvious to combine Cidon’s user “access policies” and file “placement policies” to achieve the single claimed “policy.” I am informed even though these dissimilar policies are described in the same single reference, Petitioner must still articulate a rationale for combining them. But Petitioner has not done so.

66. For claim 1 only, Petitioner also relies on Herrmann for its purported disclosure of claim 1’s separate requirement of a “gateway” that “assign[s]” policies. *See* Pet., 25-29. But Petitioner does not assert that Herrmann’s “access policy” discloses the claimed policy, or that Herrmann would have motivated a POSITA to combine Cidon’s (or Herrmann’s) disparate policies to achieve the single claimed “policy.” *See id.* And a POSITA would have understood that Herrmann clearly doesn’t. For example, Herrmann’s access policy does not define “cryptographic key information” for encrypting a file, or otherwise relate in anyway way to “processing”

and “storing” a file on the cloud. In fact, as discussed above (and further discussed below), Herrmann has nothing to do with cloud file storage policies.

67. Overall, Petitioner appears to completely ignore or overlook the fact that the Petition relies on multiple dissimilar policies to address the single “policy” recited by the independent claims.

**B. The Petition Fails to Show the References Render Obvious
“Encrypting ... Content of the File to Produce a Searchable
Encrypted File”**

68. Independent claim 1 recites “encrypting ... content of the file to produce a searchable encrypted file.” Ex. 1001, claim 1[c]. Similarly, independent claim 16 recites “produc[ing] a searchable encrypted file by encrypting content of the file.” *Id.*, claim 16[c][ii][A]. For both these claim elements, Petitioner relies solely on Cidon, which Petitioner argues “taught or suggested that [its] encrypted files were searchable.” Pet. 32-33, 54. As discussed below, I disagree.

69. First of all, a POSITA would have understood that encrypting content of a file to produce a “searchable encrypted file” (i.e., an encrypted file whose contents can still be searched) was highly unconventional at the time of the priority date for the ’678 patent. At that time, all conventional encryption methods produced encrypted files that were not searchable (i.e., encrypted files whose contents could not be searched). In my opinion, if Cidon had intended to teach or suggest an encryption process that produced a “searchable encrypted file,” Cidon would have

clearly said so, especially given that Cidon is specifically directed to a system and methods for encrypting files. But a POSITA would have understood that Cidon never discloses a searchable encryption process.

70. Petitioner asserts that Cidon “taught or suggested [its] encrypted files were searchable” because Cidon discloses functions for “[a]ccessing the complete user file and folder structure by browsing the web service account ... [and] functionalities such as document search.” Pet. 32-33; Cidon, ¶¶89-91. But a POSITA would have understood that this portion of Cidon does not teach or suggest that the contents of Cidon’s encrypted documents are searchable. Instead, a POSITA would have understood that this portion of Cidon describes system management functions that enable users to find documents in the system (e.g., by performing a “document search” or browsing the system’s “file and folder structure” for a document with a particular filename). Cidon, ¶91. And a POSITA would have understood that the ability to search for and find files in a system is distinctly different from the ability to search the contents of the files themselves, which requires a specific type of encryption algorithm and search infrastructure that certainly would have merited at least a passing reference in Cidon if it had intended to incorporate this kind of technology. Once again, at the time of the ’678 patent (and up to the present time), conventional encryption systems *overwhelmingly* do not include the ability to search encrypted contents.

71. Petitioner also asserts that Cidon describes extracting metadata from files that “may help in file search operation, using text/tags based search or one or more document references.” Pet. 32; Cidon, ¶¶166, 171. But a POSITA would have understood that this portion of Cidon also does not teach or suggest that the contents of Cidon’s encrypted documents are searchable. Instead, a POSITA would have understood that this portion of Cidon describes the use of metadata to find and identify files in the system (e.g., by searching metadata text and/or tags for a particular filename). Cidon, ¶¶165-171. And, as discussed above, a POSITA would have understood that the ability to search for and find files in a system is distinctly different from the ability to search the contents of the files themselves.

72. Finally, and importantly, a POSITA would have understood that neither of the disclosures Petitioner identifies in Cidon even refers to searching encrypted documents or files. *See* Cidon, ¶¶91, 166, 171. Consequently, and given Cidon teaches that only some files are encrypted (*see, e.g., id.* ¶¶224-228), a POSITA would have understood that the identified disclosures do not refer to search operations performed on the contents of encrypted documents or files. Indeed, a POSITA would have understood that there is no disclosure anywhere in Cidon that teaches or suggests its encrypted documents or files are searchable.

73. For all these reasons, it is my opinion that Petitioner has not shown that Cidon teaches, suggests, or renders obvious producing a “searchable encrypted file” as recited by the independent claims.

C. The Petition Fails to Establish or Sufficiently Explain the Alleged Combination of Cidon With Shikfa

74. Independent claims 1 and 16 both recite a process for producing a searchable encrypted file that involves: “divid[ing] [a] file into [] chunks; creat[ing] namespaces for one or more of the [] chunks; and configur[ing] the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.” Ex. 1001, claims 1[b][i]-[iii], 16[c][ii][B]-[D].

75. Petitioner acknowledges that Cidon does not disclose at least the last part of this process. *See* Pet. 40 (“Cidon ... did not explicitly disclose configuring the segment identifiers (namespaces) so the file content was encrypted in a searchable manner.”); 55 (citing back). And I agree. But Petitioner asserts that a POSITA “would have been motivated to combine Shikfa’s searchable encryption mechanism with Cidon’s encryption technique.” Pet. 43-44, 55. In my opinion, for the reasons discussed below, Petitioner has not shown such a motivation and, in fact, it is my opinion that a POSITA would not have been motivated to combine Shikfa and Cidon in this manner.

76. First of all, Cidon teaches that its “management server” is already a “complete software system which is responsible for encrypting files in the cloud and

enforcing secure access to these cloud files.” Cidon, ¶102. And Cidon already describes a detailed and comprehensive set of file encryption methods implemented by this management server. *See, e.g., id.*, ¶¶234-402. Given these teachings, Petitioner does not show or explain why a POSITA would have been motivated to modify Cidon’s “complete” system with just this one piece of Shikfa’s encryption method (i.e., Shikfa’s alleged configuration of identifiers), rather than simply using the complete set of encryption methods that Cidon already discloses. In my opinion, a POSITA would not have had any motivation to make the proposed modification. Instead, the only motivation is hindsight.

77. Petitioner asserts that the “modified system would have been benefitted from various advantages that Shikfa described,” including that “the system would have allowed file content to be encrypted and searched ‘without requiring any such capability’ at a storage provider.” Pet. 44 (citing Shikfa, ¶50); *see also* Pet. 22 (identifying the same purported benefit). But a POSITA would have understood that Cidon’s system already provides for encryption of file content without requiring that capability at the storage provider. In fact, that is one of the primary purposes of Cidon’s system. *See* Cidon, Abstract, ¶¶97-99, 218-223. Moreover, at least according to Petitioner, Cidon’s system also already provides for “searchable encryption” (but as discussed above, I disagree). Pet. 21, 32-33. This purported

benefit is something that Cidon purportedly already provides, and it would not have provided a motivation to combine with Shikfa.

78. Petitioner also asserts that “the modified system would have ‘accommodate[d] document searchability’ without ‘compromis[ing the] ... privacy needs,’ thereby protecting confidential information.” Pet. 44 (citing Shikfa, ¶50). But in my opinion, a POSITA would have understood that this aspect of Shikfa actually teaches against Petitioner’s purported combination. As I discussed earlier, although Shikfa’s system includes an intermediary “broker server” that “transfer[s] [] encrypted documents between the client and the [] storage providers” (Shikfa, Abstract), Shikfa expressly teaches that only the client “encrypts the [] documents” (*id.*, ¶29), “ensur[ing] that the broker server 12 cannot access and/or discover the content of the client’s data.” *Id.*, ¶48. This directly contrasts with the ’678 patent, which, as I discussed earlier, teaches that its searchable encryption processes are implemented at its intermediary Gateway system, and not at the client. For these reasons, a POSITA would have understood that to fulfill Shikfa’s stated privacy needs, Shikfa’s encryption techniques should not be implemented on an intermediary gateway system (as the ’678 patent’s claims require), or on the server systems disclosed in Cidon (and in Herrmann).

79. In my opinion, for all these reasons, Petitioner has not shown that a POSITA would have been motivated to combine the one identified piece of Shikfa’s

encryption technique (i.e., Shikfa’s purported configuration of identifiers) with the comprehensive encryption methods already disclosed in Cidon’s “complete” system (or the server systems disclosed in Herrmann), let alone to combine them in the specific manner of the ’678 patent’s claims. As discussed above, if anything, a POSITA would have understood that Shikfa teaches away from the combination.

80. In my opinion, Petitioner also does not show that POSITA would have had a reasonable expectation of success. Petitioner contends that a POSITA would have reasonably expected success “because searchable encryption mechanisms had been well-known and would have been compatible with Cidon and Herrmann’s systems, and the combination would have yielded expected results.” Pet. 45. But a POSITA would have understood that searchable encryption is an extremely complex technology, and that it was highly unconventional at the time of the invention. Moreover, a POSITA would have viewed Shikfa’s searchable encryption technique as incompatible with Cidon’s system, including because Cidon’s “management server” is already a “complete software system” performing encryption methods that encrypt individual “file segments.” Cidon, Abstract, ¶¶10, 102. In contrast, Shikfa’s encryption technique is performed on entire documents and is not intended to be performed on server systems like that of Cidon (or Herrmann). *See* Shikfa, ¶¶29, 48. Given these critical differences, Petitioner has not shown that a POSITA would

have had a reasonable expectation of success in combining these references, let alone in the specific manner of the '678 patent's claims.

81. For all these reasons, it is my opinion that Petitioner does not show a POSITA would have had a motivation to combine and reasonable expectation of success in combining Shikfa with Cidon to achieve the claim limitation that recites “configur[ing] the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.”

D. The Petition Fails to Establish or Sufficiently Explain the Alleged Combination of Cidon/Shikfa With Herrmann

82. Independent claim 1 recites that multiple different claim steps (including “assigning,” “encrypting,” and “storing”) are performed “by a gateway device.” Ex. 1001, claim 1. Petitioner acknowledges that, at the least, Cidon does not disclose that the claimed “assigning” step is performed “by a gateway device.” *See* Pet. 25 (“Cidon ... did not explicitly disclose assigning such a policy ‘*by a gateway device.*’”). And I agree. But Petitioner alleges that a POSITA “would have added Herrmann’s gateway server and its access policy assignment functionality to Cidon’s management server.” Pet. 27; *see also id.* 21-22, 25-30, 44-46 (referring to the alleged Cidon/Shikfa/Herrmann combination for multiple claim steps). In my opinion, for the reasons discussed below, Petitioner has not shown a motivation to combine or reasonable expectation of success and, in fact, a POSITA would not have been motivated or reasonably expected success in making the proposed combination.

83. First of all, importantly, Petitioner does not even consistently articulate the proposed combination. In some cases, Petitioner asserts the combination would have “would have added Herrmann’s gateway server ... to Cidon’s management server.” Pet. 27; *see also id.* 22 (“incorporating Herrmann’s techniques to Cidon’s system”). But in other cases, Petitioner asserts the same purported combination “would have entailed implementing Cidon’s [management server operations] on Herrmann’s gateway device.” *Id.* 21-22; *see also id.* 29 (“Herrmann’s gateway server could have accommodated Cidon’s management server operations”).

84. Second of all, I note that Petitioner does not identify a motivation to combine the references (or reasonable expectation of success) for each of the applicable claim steps. For example, for the claim step requiring “storing, by the gateway device, the searchable encrypted file,” Petitioner asserts that “[i]n the Cidon-Herrmann-Shikfa combination, the gateway device including the functionality of Cidon’s management server would store the encrypted files on a cloud platform based on the policy.” Pet. 46. But Petitioner does not assert any motivation or rationale for combining the different references in the specific manner required by this claimed “storing” step. *See also id.* 29-30 (another example).

85. In my opinion, Petitioner does not show any motivation to combine Cidon with Herrmann. As I discussed earlier, Cidon teaches that its “management server” is already a “complete software system which is responsible for encrypting

files in the cloud and enforcing secure access to these cloud files.” Cidon, ¶¶102. Moreover, in this capacity, Cidon’s management server is already “connected to consumer-based file repositories” and can already “communicate with user devices.” *Id.*, ¶¶100-102, Fig. 2. Consequently, a POSITA would not have been motivated to modify Cidon’s already “complete” system to incorporate Herrmann’s gateway server, given that Cidon’s management server is already capable of performing all of these communication functions.

86. In addition, a POSITA would not have been motivated to make the proposed combination because Cidon and Herrmann are non-analogous references in different fields of art. A POSITA would have understood that Cidon teaches a complete server system that encrypts and stores files in the cloud and then controls user access to those files. Cidon, ¶¶10, 102, Fig. 2. In contrast, Herrmann teaches a gateway system that enforces the installation and use of approved anti-virus applications on client computers before they can access a network or other protected resources. Herrmann, ¶¶29, 50, Figs. 3-4. Importantly, as I discussed earlier, Herrmann does not disclose using its anti-virus enforcement system in connection with encrypting, storing, or controlling user access to files stored in the cloud. In fact, a POSITA would have understood that Herrmann does not address cloud storage at all. In my opinion, for all these reasons, a POSITA would not have looked

to Herrmann's gateway server to modify Cidon's complete system focused on encrypting files in cloud storage.

87. Petitioner contends that a POSITA would have been motivated to combine Cidon with Herrmann "because instead of waiting for an administrator to assign a policy manually, the modified system would have allowed automatic policy assignment and implementation." Pet. 28; *see also* Pet. 22 (identifying the same purported benefit of the combination). But a POSITA would have understood that Herrmann's gateway server only "assigns an access policy to the connection/session between the gateway server 350 and the client computer" after its separate "integrity server" determines that the client computer is in compliance with applicable anti-virus rules. Herrmann, ¶¶60, 77. For at least this reason, a POSITA would not have looked to Herrmann's gateway server's automatic policy assignment to improve Cidon's system, which has no "integrity server," and which must assign its policies before any compliance determinations are made regarding access to secure files. *See, e.g.*, Cidon, ¶¶108-109. For all these reasons, a POSITA would have had no motivation to combine Cidon (and Shikfa) with Herrmann, let alone in the specific manner of challenged claim 1.

88. In my opinion, Petitioner also does not show that a POSITA would have had a reasonable expectation of success. Petitioner asserts that "[t]his combination would have been straightforward because gateway devices were well-known for

network security-related functionalities” and because Herrmann’s gateway server allegedly “could have accommodated Cidon’s management server operations and yielded predictable results.” Pet. 28-29. But a POSITA would have understood that Cidon’s “management server” was already a “complete software system” that would have been incompatible with Herrmann’s gateway server, which requires a separate “integrity server” to even properly function. And a POSITA would have further understood that Herrmann’s simple gateway server could not have accommodated Cidon’s complicated file encryption, storage, and access control operations, or the complex searchable encryption techniques taught in Shikfa.

89. For all these reasons, it is my opinion that Petitioner does not show a POSITA would have had a motivation to combine and reasonable expectation of success in combining Cidon and Shikfa with Herrmann to meet the “assigning,” “encrypting,” and “storing” steps of claim 1.

E. The Petition Fails to Show the References Render Obvious “A Policy Selected From a Group of Policies”

90. Independent claim 16 requires implementing “a policy selected from a group of policies for a user.” Ex. 1001, claim 16[c][i]. For this element of claim 16, Petitioner relies exclusively on Cidon, asserting that “it would have been obvious to a POSITA that Cidon’s IT policy enforcement module would select a policy for the appropriate user/group” because, according to Petitioner, “Cidon described that

different users/groups were assigned different policies.” Pet. 53 (citing Cidon, ¶108). For the reasons discussed below, I disagree.

91. First of all, a POSITA would have understood Cidon never discloses that different users/groups are assigned different policies. Instead, Cidon discloses that an “administrator” (i.e., a person) “define[s] access policies” for users “through a web browser interface.” Cidon, ¶108. And a POSITA would have understood that defining a policy is clearly different than “select[ing] [a policy] from a group of policies.” For example, defining a policy involves specifying a new policy, whereas selecting a policy from a group of policies does not. In addition, in light of Cidon expressly teaching that its policies are defined by an “administrator” (i.e., a person), a POSITA would not have found it obvious that Cidon’s IT policy enforcement module would, instead, define (or assign, or select) those policies.

92. In my opinion, Petitioner does not provide any reasonable rationale for why a POSITA would have found it obvious that Cidon’s IT policy enforcement module would “select[] [a policy] from a group of policies for a user,” as challenged claim 16 requires. In fact, in light of Cidon’s explicit teaching to the contrary, this would not have been obvious to a POSITA.

VII. GROUNDS 2 AND 3 FAIL FOR THE SAME REASONS THAT GROUND 1 FAILS

93. Grounds 2 and 3 of the petition challenge dependent claims that depend from claims 1 or 16. Thus, they rely on the analysis of Ground 1. In my opinion,

Grounds 2 and 4 fail for the same reasons that I discussed above in connection with Ground 1.

VIII. THE PETITION FAILS TO SHOW THAT AURADKAR, CHIUEH, AND CHAMBERS RENDER CLAIMS 1-3, 8-19, AND 21-27 OBVIOUS (GROUND 4)

A. The Petition Fails to Show the References Render Obvious the “Policy for Managing Access to and Processing a File”

94. As I discussed earlier in connection with Ground 1, independent claims 1 and 16 both recite a single “policy for managing access to and processing a file” (or similar), along with a number of other claim requirements regarding the same “policy.” *See* Ex. 1001, claims 1, 16.

95. As it did with Ground 1, Petitioner once again completely ignores or overlooks that the claims recite only a single “policy,” and Petitioner does not show that the references in Ground 4 disclose or render obvious a single “policy” that meets all the claim requirements. Instead, Petitioner points to several very different policies in Auradkar, incorrectly treating them as if they were the same policy. Petitioner does not show or even allege that these different policies are the same single “policy” as required by the claims, or that it would have been obvious to combine Auradkar’s policies into the single claimed policy.

96. For example, in asserting that Auradkar “disclosed that its policy defined user access rights,” Petitioner points only to Auradkar’s disclosure of “access policies” (e.g., “enterprise access policy 530”) that control user access to

data. *See* Pet. 87-88 (discussing Auradkar, ¶¶112, 117); Pet. 116 (citing back). However, in asserting that Auradkar also “disclosed [] storing the searchable encrypted file ... based on the policy,” Petitioner instead points only to Auradkar’s separate disclosure of data storage policies that control “how [and] where [data] could be stored.” *See* Pet. 106-107 (discussing Auradkar, ¶¶96, 130, Fig. 15); Pet. 117 (citing back). And this pattern of mixing and matching of Auradkar’s dissimilar policies occurs throughout the fourth ground of the petition. *See* Pet. 80-83, 87-88, 92-93, 106-109, 115-118.

97. A POSITA would have understood that Auradkar’s “access policies” and data storage policies are completely different. First, “an enterprise 620 defines its enterprise access policy 630 applicable to enterprise staff.” Auradkar, ¶119. In contrast, Auradkar’s data storage policies are “create[d] ... [for] data.” *Id.*, ¶96. Second, “access policies” govern whether different “users seek[ing] access to [protected] data ... [are] allow[ed] or den[ied] entry.” *Id.*, ¶116. In contrast, Auradkar’s data storage policies are used to implement data storage restrictions controlling “how data could be stored, where it could be stored, how long it could be stored, etc.” *Id.*, ¶96. In addition, a POSITA would have recognized that Auradkar discusses its “access policies” and data storage policies in different portions of the reference, and that Auradkar never says they are related.

98. Importantly, Petitioner does not show or allege that a POSITA would have understood Auradkar's "access policies" and data storage policies to be the same single "policy" required by the claims. And, as discussed above, it is my opinion that a POSITA would not have understood them to be the same policy.

99. Petitioner also does not show or allege that it would have been obvious to combine Auradkar's "access policies" and data storage policies to achieve the single claimed "policy." As I discussed earlier, I am informed even though these dissimilar policies are described in the same single reference, Petitioner must still articulate a rationale for combining them. But Petitioner has not done so.

100. Petitioner relies on Chambers for its purported disclosure of a "gateway" (claim 1) and "access control module" (claim 16). *See* Pet., 83-87, 115-116. But Petitioner does not assert that Chambers discloses the claimed policy, or that Chambers would have motivated a POSITA to combine Auradkar's (or Chambers') disparate policies to achieve the single claimed "policy." *See id.* And a POSITA would have understood that Chambers clearly doesn't. Chambers does not disclose a policy that defines "cryptographic key information" for encrypting a file, or otherwise relate in anyway way to "processing" and "storing" a file on the cloud. As discussed above (and further discussed below), Chambers has nothing to do with cloud file storage policies.

101. Overall, Petitioner once again appears to completely ignore or overlook the fact that the Petition relies on multiple dissimilar policies in Auradkar to address the single “policy” recited by the independent claims.

B. The Petition Fails to Establish or Sufficiently Explain the Alleged Combination of Auradkar With Chiueh

102. As I discussed earlier in connection with Ground 1, independent claims 1 and 16 both recite a process for producing a searchable encrypted file that involves: “divid[ing] [a] file into [] chunks; creat[ing] namespaces for one or more of the [] chunks; and configur[ing] the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.” *See* Ex. 1001, claims 1[b][i]-[iii], 16[c][ii][B]-[D].

103. Petitioner recognizes that Auradkar does not disclose this complete process (and I agree), but Petitioner contends that Auradkar combined with Chiueh disclose the second and third parts of this process. *See* Pet. 94, 98, 117. More specifically, Petitioner contends that a POSITA “would have been motivated to modify [Auradkar’s] technique by Chiueh’s mechanism that allowed searching individual document pages.” *Id.* 79; *see also id.* 97, 106 (more discussion of the same alleged combination). But as I discussed below, Petitioner does not show that a POSITA would have had any motivation to make this combination, or that a POSITA would have had a reasonable expectation of success.

104. First, as a basis for the motivation to combine these references, Petitioner cites to Dr. Lee at ¶¶185-187, and then more or less repeats Dr. Lee's bases for the motivation to combine Auradkar, Chiueh and Chambers. Dr. Lee opines that a POSITA would have been motivated to combine these references because "all these references were concerned with improving computer networking and security for accessing files stored in a remote site from client devices." But such a broad objective (secure access by client devices of remote files) describes virtually any client-server system in existence. Indeed, a primary objective of the world-wide web is providing secure access by browsers (clients) to files (HTML, CSS, Javascript, PDF documents, etc) stored on a remote system (a web server). Virtually any networked computer system in existence has this goal and it hardly provides a basis for focusing on just these three references as Dr. Lee does. Dr. Lee also opines that a POSITA would have been motivated to combine these references because the combination "would have also produced a better system." Dr. Lee justifies this claim by using virtually the same language from the '678 Patent when it describes the advantages embodied in the invention: that searchable encryption allows searching portions of a document rather than the whole document. But such reasoning is plainly hindsight and not a proper motivation to combine references. There are further flaws in Petitioner's motivation to combine references, as I explain below.

105. Second, Petitioner’s proposed combination would “combine Auradkar, Chiueh, and Chambers,” and would “incorporat[e] Chambers’ dedicated gateway as an interface between the client and protected data sources” (Pet. 78-79) “such that the claimed operations would be carried out by the gateway.” *Id.* 93; *see also id.* 85, 108, 115-116. But a POSITA would have understood that Chiueh teaches against this proposed combination. Chiueh clearly teaches that only the client “encrypts the document pages and the significant word set” so that “remote server[s] do[] not have the keys [and can] not decrypt the document pages and the significant word set.” Chiueh, ¶¶8-10; *see also* ¶5. As I discussed earlier, this teaching directly contrasts with the ’678 patent, which teaches that its searchable encryption processes (and other process) are implemented at its Gateway system, and not at the client. In my opinion, given Chiueh’s clear teachings to the contrary, a POSITA would have understood that Chiueh’s encryption techniques should not be implemented on an intermediary gateway system (as the ’678 patent claims require), or on the remote systems disclosed in Chambers and Auradkar.

106. Petitioner contends that a POSITA would have been motivated to make the proposed modification “because, in addition to Auradkar’s existing whole-document search, the modified system would have allowed retrieval of encrypted document portions stored in the cloud.” Pet. 97; *see also* Pet. 79, 106 (identifying the same alleged benefit of the proposed combination). But Auradkar’s “trustworthy

platform” already purportedly allows for search and retrieval of encrypted document portions stored in the cloud. Petitioner alleges Auradkar provides for “searchable encryption” of documents. And Auradkar’s search techniques allow data to be “selectively queried to obtain access to XML fragments” constituting “sliver[s] of a larger document ... dispersed across different [cloud storage] containers.” Auradkar, ¶¶91-92; *see also id.*, ¶¶93-95 (Auradkar’s platform “enable[s] users to search, extract and decrypt segments, subsets or parts of encrypted data,” such as individual “paragraphs” of an “XML document”). For these reasons, the purported benefit Petitioner identifies is something that Auradkar allegedly already offers. It would not have provided a POSITA a motivation to combine to combine the references, let alone in the specific manner of the claims.

107. In my opinion, Petitioner does not identify any valid reason why a POSITA would have been motivated to modify the searchable encryption techniques already included in Auradkar’s comprehensive platform with individual pieces of Chiueh’s encryption technique, let alone in the specific manner of the ’678 patent’s claims. In fact, a POSITA would not have had any motivation to make this combination at the time of the invention. The only motivation is hindsight.

108. In my opinion, Petitioner also does not show that a POSITA would have had a reasonable expectation of success. Petitioner contends that a POSITA would have reasonably expected success “because Auradkar already disclosed generating

tags, which could include filenames for payloads, and using these tags to search the encrypted payloads.” Pet. 97; *see also* Pet. 106 (citing back). But a POSITA would have understood that Auradkar and Chiueh each teach their own complex searchable encryption techniques, and that those techniques are different. Auradkar disclosed techniques using tags containing metadata. *See, e.g.*, Auradkar, ¶¶90. That does not mean those techniques could have been modified with Chiueh’s very different page-based “significant-word-set” technique (*see, e.g.*, Chiueh, ¶¶8-9), let alone modified in the specific manner of the ’678 patent’s claims. In my opinion, a POSITA would not have reasonably expected success in making the proposed combination.

109. Petitioner also contends that “creating identifiers for portions of a document had been well-known, would have been compatible with Auradkar’s system, and the combination would have yielded expected results.” Pet. 97. As discussed above, I disagree. And while creating identifiers was known at general level, that does not mean a POSITA would have reasonably expected success in modifying the specific searchable encryption techniques in Auradkar’s platform with Chiueh’s very different technique. In my opinion, they are incompatible.

110. Petitioner also does not show that a POSITA would have had a motivation to combine or a reasonable expectation of success in implementing the identified portions of Chiueh’s searchable encryption technique on Chambers’ gateway system, which Petitioner’s overall proposed combination would require. As

a discussed earlier, Chiueh expressly teaches its technique should only be performed by the client, and not on remote systems like Chambers' gateway. *See* Chiueh, ¶¶5, 8-10. Consequently, a POSITA would not have been motivated to make this proposed combination, or had a reasonable expectation of success.

111. For all these reasons, it is my opinion that Petitioner does not show a POSITA would have had a motivation to combine and reasonable expectation of success in combining Chiueh with Aradkar and Chambers to achieve the claim limitations requiring “creat[ing] namespaces for one or more of the [] chunks” and “configur[ing] the namespaces of the one or more chunks such that content of the file is encrypted in a manner that makes it searchable.”

C. The Petition Fails to Establish or Sufficiently Explain the Alleged Combination of Auradkar/Chiueh With Chambers

112. As I discussed earlier in connection with Ground 1, independent claim 1 recites that multiple claim steps (including “assigning,” “encrypting,” and “storing”) are performed “by a gateway device.” *See* Ex. 1001, claim 1. Petitioner recognizes that, at the least, Auradkar does not disclose that the claimed “assigning” step is performed “by a gateway device.” *See* Pet. 83 (“Auradkar ... did not explicitly disclose a *gateway device* assigning the policy”). And I agree.

113. Independent claim 16 recites multiple stored modules (including “a policy assignment module,” “an encryption module,” “a storage module,” and “a management module”) that each perform claimed processes. Ex. 1001, claim 16.

Here, Petitioner implicitly concedes that, at the least, Auradkar fails to disclose the claimed “policy assignment module.” *See* Pet. 115-116. Once again, I agree.

114. To address these gaps, Petitioner asserts that a POSITA would have “incorporat[ed] Chambers’ dedicated gateway as an interface between the client and protected data sources” (Pet. 79) and “use[d] Chambers’ gateway to implement Auradkar’s ‘assigning’ function (and other claimed functions), and to automatically assign the pertinent security policies.” *Id.* 85; *see also id.* 93, 108, 115-116 (referring to the same purported combination in connection with multiple claim limitations). But as I discussed below, Petitioner does not show that a POSITA would have had any motivation to make this combination, or that a POSITA would have had a reasonable expectation of success.

115. First of all, importantly, Petitioner does not identify a motivation to combine the references (or reasonable expectation of success) for each of the applicable claim elements. For example, for the claim step requiring “storing, by the gateway device, the searchable encrypted file,” Petitioner asserts that “a POSITA would have found it obvious to use Chambers’ gateway device to perform the functions described in Auradkar, such as storing the searchable encryption file on one or more cloud platforms based on the policy.” Pet. 108. But then, for support, Petitioner just refers back to a prior section discussing the “assigning” claim step, which is very different. Petitioner does not identify any motivation for combining

the references in the specific manner required by the claimed “storing” step. *Id.*; *see also id.* 93 (another example). And Petitioner’s assertions in connection with claim 16 are similarly lacking. *See, e.g., id.* 117 (“A POSITA would have found it obvious that Auradkar’s system would have included various modules, including the claimed ‘encryption module,’ that would be executed by its processing unit (processor)”) (citing back); *see also id.* 115-118 (other examples).

116. In my opinion, Petitioner does not show any motivation to combine Auradkar (and Chiueh) with Chambers. As I discussed earlier, a POSITA would have understood that Auradkar already discloses a comprehensive “trustworthy platform” using “mathematical transformation techniques, such as searchable encryption, deassembling/reassembling or distribution techniques,” to “distribute[] trust across multiple entities ... and decouple[] data protection requirements ... from the containers that hold the data (e.g., file systems, databases, etc.) enabling the data to act as its own custodian through imposition of a shroud of mathematical complexity.” Auradkar, ¶¶9-13. Given these teachings, Petitioner does not explain how or why a POSITA would look to modify Auradkar’s platform to implement Auradkar’s complex techniques on Chambers’ simple “network access device” (i.e., the purported “gateway” device), which cannot even function properly without a separate “management server.” *See* Chambers, ¶¶24-28. In fact, a POSITA would have understood that Chambers’ simple network access device would be incapable

of implementing Auradkar's complex techniques, making the proposed combination unworkable. And given that Auradkar already provides a comprehensive platform, a POSITA would have had no motivation to even attempt the combination.

117. In my opinion, a POSITA also would not have been motivated to make the purported combination because Auradkar and Chambers are non-analogous references in different fields of art. A POSITA would have understood that Auradkar teaches a comprehensive "trustworthy platform" that uses complex mathematical techniques to provide "containerless" protection of data stored by cloud services in a system of "distribute[d] trust." Auradkar, Abstract, ¶¶9-13. In contrast, Chambers teaches using "network access devices" to "automatically assign[] [network] access control policies (ACPs) based on [client] device types," where the policies specify network parameters such as "bandwidth limits and traffic shaping rules, VLAN assignment, firewall rules, whether a captive portal should be applied to that device, etc." Chambers, ¶¶21, 24-28, 32-40. As I discussed earlier, a POSITA would have understood that Chambers does not disclose using its network access control techniques in connection with encrypting, storing, or controlling access to files stored in the cloud. In fact, a POSITA would have understood that Chambers does not address cloud storage at all. For all these reasons, a POSITA would not have looked to Chambers' simple network access device to modify Auradkar's comprehensive platform.

118. Petitioner contends that a POSITA would have been motivated to “incorporat[e] Chambers’ dedicated gateway as an interface between the client and protected data sources [because this] would have enhanced network security by, e.g., shielding these sources from the client.” Pet. 79; *see also* Pet. 87 (identifying the same purported benefit of the proposed combination). But one of Auradkar’s central goals is actually to “[e]liminat[e] [] external entity controlled active custodianships” of data and, instead, “provide a system where data ... acts as a custodian for itself regardless of the third party machine(s), mechanism(s), device(s) or container(s) holding the data,” and “enable containerless data along with guarantees of security, confidentiality, tamper-proof, etc., which are made transparent to the user.” Auradkar, ¶¶68-70. For this reason, a POSITA would have had no motivation to incorporate and implement Auradkar’s techniques on Chambers’ network access device, which would have only added a further and unnecessary layer of complexity.

119. Petitioner also contends that a POSITA would have been motivated to “[i]ncorporat[e] Chambers’ teachings into Auradkar’s system [because this] would have allowed automatic assignment of a policy based on, e.g., a user’s role in the organization, or the user’s devices.” Pet. 86-87. But a POSITA would have understood that Chambers’ network access device only assigns policies that specify network parameters such as “bandwidth limits and traffic shaping rules, VLAN assignment, firewall rules, whether a captive portal should be applied to that device,

etc.,” and that it can only assign those policies under the control of a separate “management server.” Chambers, ¶¶24-28, 32-40. Consequently, a POSITA would not have looked to Chambers’ network access device’s automatic policy assignment to improve Auradkar’s system, which has no such separate “management server,” and which implements access policies to control users’ “access to data.” Auradkar, ¶¶116-117. For all of these reasons, a POSITA would have had no motivation to combine Auradkar (and Chiueh) with Chambers’ network access device.

120. Petitioner also does not show that a POSITA would have had a reasonable expectation of success in making the proposed combination. Petitioner asserts that a POSITA “would have reasonably expected success in making this combination because gateway devices were well-known for network security-related functionality, including controlling network traffic and managing access policies” and “adding Chambers’ gateway into Auradkar’s system would have yielded predictable results.” Pet. 87. I disagree.

121. First of all, while gateway devices may have been known for conventional network security functions, that is irrelevant here. As I discussed earlier, conventional network security is not the subject of Auradkar’s system, and Chambers’ network access control policies are very different from the user access policies at issue in Auradkar.

122. Second of all, as I discussed earlier, Auradkar already taught a comprehensive platform that would have been incompatible with Chambers' simple network access device, which requires a separate "management server" to function. Chambers' simple network access device could not have accommodated Auradkar's complicated searchable encryption, storage, and access control techniques, or the complex searchable encryption technique taught in Chiueh. Petitioner does not show how all these teachings could be successfully combined.

123. For all these reasons, it is my opinion that Petitioner does not show a POSITA would have had a motivation to combine and reasonable expectation of success in combining Auradkar and Chiueh with Chambers to meet the "assigning," "encrypting," and "storing" steps of claim 1 or the recited "module[s]" in claim 16.

IX. GROUND 5 FAILS FOR THE SAME REASONS THAT GROUND 4 FAILS

124. Ground 5 of the petition challenges dependent claims that depend from claims 1 or 16. Thus, it relies on the analysis of Ground 4. In my opinion, Ground 5 fails for the same reasons that I discussed above in connection with Ground 4.

X. CONCLUSION

125. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in the case and that cross-examination will take place within the

United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

126. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on the information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed: June 20, 2023

A handwritten signature in black ink, appearing to read 'John Black Jr.', written over a horizontal line.

John Black Jr., Ph.D.