Trials@uspto.gov
571-272-7822

Paper 12
Date: May 17, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

VIRTRU CORPORATION,
Patent Owner.

IPR2023-00019
Patent 9,578,021 B2

Before WILLIAM V. SAINDON, BENJAMIN D. M. WOOD, and SEAN P. O'HANLON, *Administrative Patent Judges*.

O'HANLON, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

Microsoft Corporation ("Petitioner") filed a Petition for *inter partes* review of claims 1–5 ("the challenged claims") of U.S. Patent No. 9,578,021 B2 (Ex. 1011, "the '021 patent"). Paper 2 ("Pet."), 1. Virtru Corporation ("Patent Owner") filed a Preliminary Response. Paper 8 ("Prelim. Resp."). With our authorization (*see* Paper 9), Petitioner filed a Preliminary Reply (Paper 10, "Prelim. Reply") and Patent Owner filed a Preliminary Sur-reply (Paper 11, "Prelim. Sur-reply").

Institution of an *inter partes* review is authorized by statute only when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a) (2018). For the reasons set forth below, upon considering the parties' briefs and the evidence of record, we conclude that the information presented in the Petition fails to establish a reasonable likelihood that Petitioner would prevail in showing the unpatentability of any of the challenged claims. Accordingly, we decline to institute *inter partes* review.

B. Real Parties in Interest

Petitioner identifies itself as the sole real party in interest. Pet. 1.

Patent Owner identifies itself as the sole real party in interest. Paper 5, 1.

C. Related Matters

The parties indicate that the '021 patent is the subject of the following district court proceeding:

> *Virtru Corp. v. Microsoft Corp.*, Case No. 6-22-cv-00242 (W.D. Tex. filed March 4, 2022) ("the Texas litigation").

Pet. 1; Paper 5, 1. The parties note other petitions for *inter partes* review filed by Petitioner and challenging patents owned by Patent Owner. Pet. 1; Paper 5, 1.

D. The Challenged Patent

The '021 patent discloses a system for distributing cryptographic data to trusted recipients. Ex. 1011, 1:25–27. The system includes an access control management system, an identity provider, and client devices. *Id.* at 8:1–5, Fig. 2C. The user of a first client device creates, for example, a document and encrypts the document to create an encrypted data object. *Id.* at 8:40–51, 9:5–9. The encryption process also generates information regarding the encrypted data object. *Id.* at 8:32–40, 9:17–20. This information is associated with the encrypted data object and includes, for example, an encryption key and an access control list that specifies which users may receive the encryption key to decrypt the data object. *Id.* at 9:20–24.

A second user desiring access to the encrypted data object sends a request for the information associated with the encrypted data object to the access control management system. Ex. 1011, 14:9–11. The access control management system first verifies that the second user is identified on the access control list. *Id.* at 11:12–15, 14:58–64. This verification may include

determining whether the information includes an identifier of the second user. *Id.* at 11:15–19. After the second user has been verified, the access control management system then identifies a third-party authentication provider implicated by the user identifier (*id.* at 13:35–42) and requests that the provider authenticate the second user (*id.* at 15:36–52). After the second user has been authenticated, the access control management system then sends the information associated with the encrypted data object to the second user, allowing the second user to decrypt the data object. *Id.* at 12:13–18, 16:54–56. Figure 3, reproduced below, depicts a flowchart of these steps.

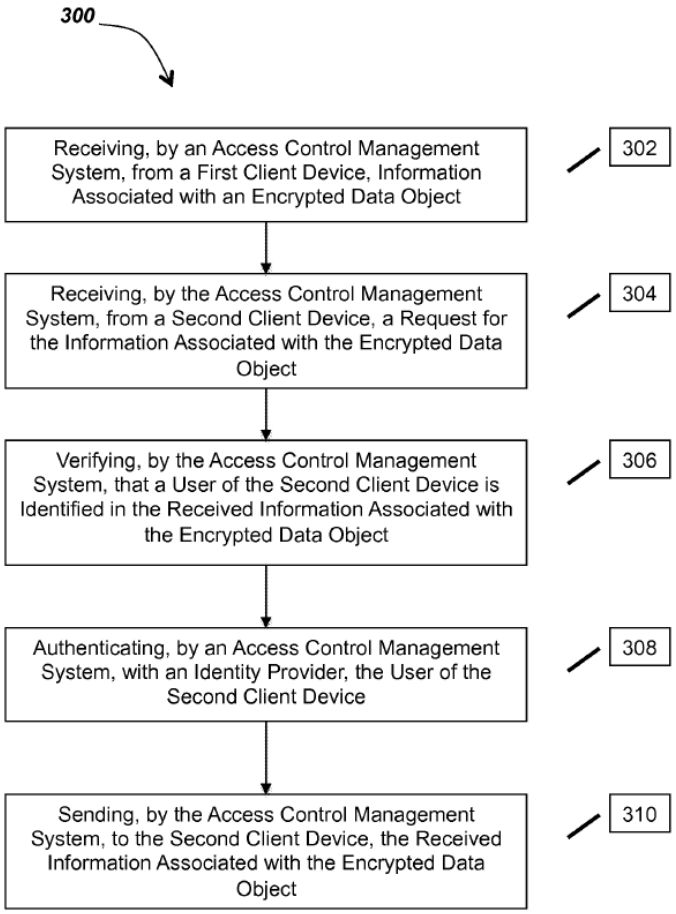


Fig. 3

Figure 3 of the '021 patent depicts a flowchart listing the steps just described. *Id.* at 3:1–3.

E. The Challenged Claims

Petitioner challenges claims 1–5 of the '021 patent. Claims 1 and 4 are independent. Claim 1 is illustrative of the challenged claims and is reproduced below.

> 1. A method comprising:
>
> receiving, by an access control management system, from a first client device, information associated with an encrypted data object;
>
> receiving, by the access control management system, from a second client device, a request for the information associated with the encrypted data object;
>
> verifying, by the access control management system, that a user of the second client device is identified in the received information associated with the encrypted data object;
>
> automatically selecting, by the access control management system, an identity provider from a plurality of identity providers, based on a user identifier included in the received information associated with the encrypted data object, the user identifier associated with the user of the second client device;
>
> automatically requesting, by the access control management system, from the selected identity provider, authentication of the user of the second client device;
>
> sending, by the access control management system, to the second client device, the received information associated with the encrypted data object, responsive to the authentication by the selected identity provider of the user of the second client device; and

storing, by the access control management system, in a transaction log, an identification of at least one of the second client device and the received request for the information.

Ex. 1011, 22:15–43.

F. Asserted Grounds of Unpatentability

The Petition relies on the following prior art references:

Name	Reference	Exhibit
Templin	US 8,898,482 B2, issued November 25, 2014	1005
McDaniel	US 9,736,153 B2, issued August 15, 2017	1007
Gilliam	US 7,206,765 B2, issued April 17, 2007	1008

Petitioner asserts the following grounds of unpatentability:

Claim(s) Challenged	35 U.S.C. §	Reference(s)
1–3	103(a)[1]	Templin
1–3	103(a)	Templin, McDaniel
4, 5	103(a)	Templin
4, 5	103(a)	Templin, McDaniel
4, 5	103(a)	Templin, McDaniel, Gilliam

Pet. 2–3. Petitioner submits a declaration of William Rosenblatt (Ex. 1002) in support of its contentions. Patent Owner submits a declaration of Eric B. Cole, Ph.D. (Ex. 2001) in support of its preliminary responses.

[1] The application resulting in the '021 patent claims priority to a date prior to the date when the Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112–29, 125 Stat. 284 (2011), took effect. Thus, we refer to the pre-AIA version of section 103.

II. DISCRETIONARY DENIAL

Patent Owner argues that we should exercise our delegated discretion under 35 U.S.C. § 314(a) to deny institution based on the Texas litigation. Prelim. Resp. 16–24; Prelim. Sur-reply 1–7. Petitioner counters that discretionary denial is not warranted in this proceeding. Pet. 51–53; Prelim. Reply 1–6.

Because we determine that Petitioner has not established a reasonable likelihood of prevailing with respect to any challenged claim, as explained in detail below, we do not reach Patent Owner's arguments that we should exercise our delegated discretion to deny institution.

III. PATENTABILITY ANALYSIS

A. Principles of Law

"In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")). Petitioner bears the burden of persuasion to prove unpatentability of each challenged claim by a preponderance of the evidence. 35 U.S.C. § 316(e). This burden never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). The Board may authorize an *inter partes* review if we determine that the information presented in the Petition and Patent Owner's Preliminary Response shows that there is a reasonable

likelihood that Petitioner will prevail with respect to at least one of the claims challenged in the petition. 35 U.S.C. § 314(a).

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) when in evidence, any objective evidence of nonobviousness.[2] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

The level of ordinary skill in the art is "a prism or lens" through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). The person of ordinary skill in the art is a hypothetical person presumed to have known the relevant art at the time of the invention. *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). In determining the level of ordinary skill in the art, we may consider certain factors, including: "(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the

[2] At this stage of the proceeding, the parties have not directed us to any such objective evidence.

technology; and (6) educational level of active workers in the field." *Best Med. Int'l, Inc. v. Elekta Inc.*, 46 F.4th 1346, 1353 (Fed. Cir. 2022) (citations omitted). "The patent's purpose can also be informative." *Id.*

Petitioner contends that a person having ordinary skill in the art at the time of the invention ("POSITA") would have had "a bachelor's degree in electrical engineering, computer engineering, computer science, or a related field, along with at least two or more years of work experience in digital rights management, information security, online identity management, or a similar field." Pet. 4 (citing Ex. 1002 ¶¶ 22–23). Petitioner asserts that "[m]ore education can supplement practical experience and vice versa." *Id.* (citing Ex. 1002 ¶¶ 22–23).

Patent Owner does not contest Petitioner's proposed definition or offer a definition of its own. *See generally* Prelim. Resp.

We find Petitioner's description to be consistent with the problems and solutions disclosed in the patent and prior art of record, and adopt it as our own for purposes of this Decision. *See, e.g.*, *In re GPAC Inc.*, 57 F.3d at 1579 (approving the determination of the level of ordinary skill in the art by appeal to the references of record).

C. Claim Construction

In an *inter partes* review, claims are construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b). "[T]he ordinary and

customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention" and "after reading the entire patent." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313, 1321 (Fed. Cir. 2005) (en banc). In addition to the specification and prosecution history, we also consider use of the terms in other claims and extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Id.* at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315. We also consider "[a]ny prior claim construction determination concerning a term of the claim in a civil action . . . that is timely made of record" in this proceeding. 37 C.F.R. § 42.100(b).

"The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'" *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (alteration in original) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Neither party identifies any claim term for construction. Pet. 7–8; Prelim. Resp. 15–16.

For purposes of this Decision, and based on the record before us, we determine that no construction of any term is necessary.

D. Overview of the Asserted Prior Art

1. Templin

Templin discloses a method of encrypting, transmitting, and decrypting a private message. Ex. 1005, 3:19–22. Figure 1 illustrates a dataflow diagram of the method and is reproduced below.

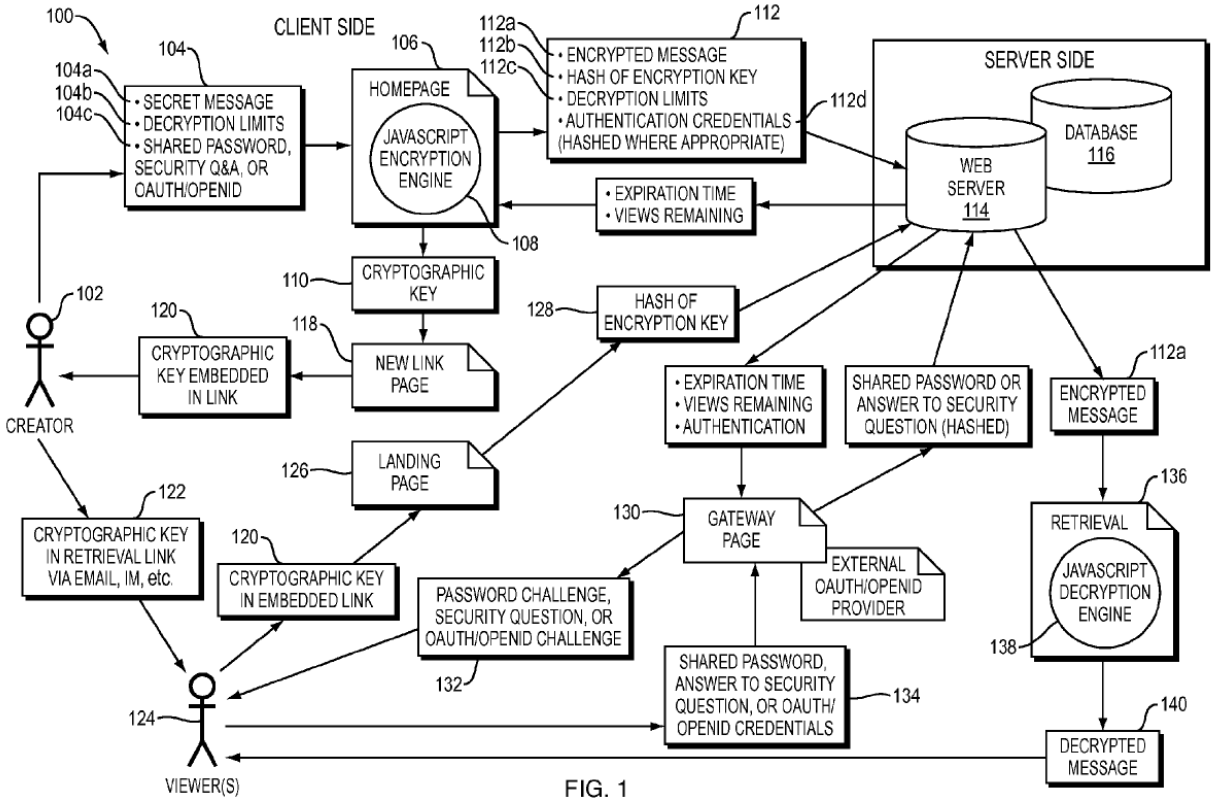


FIG. 1

Figure 1 shows a dataflow diagram of system 100 for encrypting, transmitting, and decrypting a message. *Id.* at 3:22–25. Creator 102 provides content, such as text file 104a, to be protected and system 100 encrypts the content using encryption engine 108. *Id.* at 4:55–62. In addition to producing encrypted message 112a, the encryption engine also produces cryptographic key 110. *Id.* at 5:15–18. The system transmits one of these cryptographic assets (in the illustrated example, encrypted

message 112a) and a hash of the other cryptographic asset (in this example, encryption key 110) to web server 114, and returns the other cryptographic asset (in the illustrated example, cryptographic key 110) to the creator. *Id.* at 5:18–22, 5:41–43, Fig. 1. The creator then transmits the received cryptographic asset to viewer 124. *Id.* at 6:22–27. The viewer creates a hash of the cryptographic asset and transmits the hash to the web server, which checks that it matches the hash of the cryptographic asset stored on the server. *Id.* at 6:55–7:9. The system then authenticates the viewer using authentication requirements 104c provided by the creator. *Id.* at 3:33–35, 7:46–56; *see also id.* at 3:53–4:25 (discussing authentication techniques). If the viewer is successfully authenticated, the web server transmits its stored cryptographic asset to the viewer, and the viewer uses both cryptographic assets to decrypt and access the protected content. *Id.* at 7:56–67.

2. McDaniel

McDaniel discloses methods for accessing web services using an authentication proxy to provide enhanced authentication for a client. Ex. 1007, 1:50–59. Figure 3 illustrates a dataflow diagram of the method and is reproduced below.

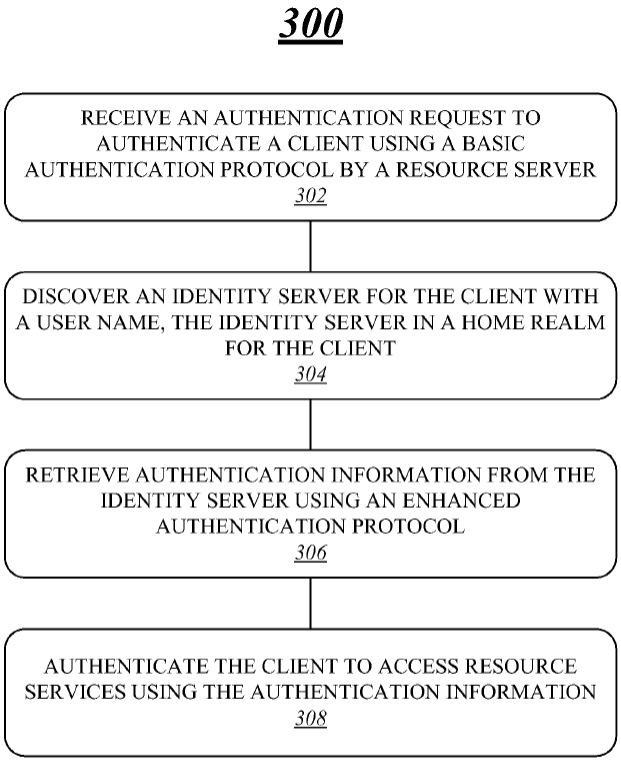


FIG. 3

Figure 3 is a flow chart that illustrates a logic flow of the authentication process. *Id.* at 13:34–37. The process begins at block 302 with a request to authenticate a user using a basic authentication protocol being received by an authentication proxy component of a resource server. *Id.* at 13:38–51. The resource server then discovers an identity server for the username included in the authentication request (block 304). *Id.* at 13:56–67. The authentication proxy component then retrieves the user's authentication information from an identity server using an enhanced authentication protocol (block 306). *Id.* at 14:1–15. The authentication proxy component then authenticates the user to access resource services using the

authentication information (block 308). *Id.* at 14:16–23. In this manner, the resource server operates as an authentication proxy for a client to access resource services requiring enhanced authentication operations without having the client upgrade to utilize the enhanced authentication protocols. *Id.* at 8:9–14.

3. Gilliam

Gilliam discloses a system for managing digital rights. Ex. 1008, 1:41–44, 3:2–5. Figure 5 illustrates a method of creating and associating usage rights and is reproduced below.

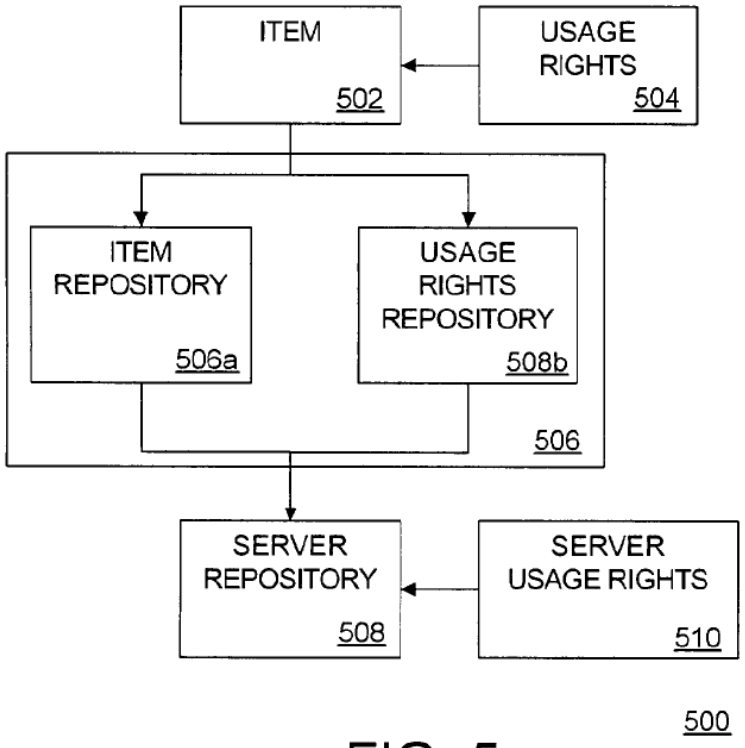


FIG. 5

Figure 5 shows digital rights management system 500. *Id.* at 14:61–63. A content creator associates usage rights 504 with digital item 502, such as a movie or song. *Id.* at 14:61–15:2. The usage rights specify the permitted

manner in which the digital item can be used, such as limiting use to a specific manner for a specified period of time. *Id.* at 5:34–39, 6:57–7:9. The item (and associated usage rights) is deposited in a client repository 506 and can be uploaded by server repository 508 if the usage rights allow. *Id.* at 15:8–27. The server repository can then use the digital item in accordance with its server usage rights 510. *Id.* at 15:23–27. Gilliam also discloses different embodiments where the usage rights are associated with an encryption key. *Id.* at 6:19–22.

E. Petitioner's Challenges

Petitioner argues that independent claim 1 would have been obvious in view of Templin, or in view of Templin and McDaniel. Pet. 2, 8–39. Petitioner applies the same analysis to independent claim 4, and also relies on Gilliam to teach a data rights protection mechanism. *Id.* at 2–3, 44–50. We have reviewed Petitioner's assertions and supporting evidence. For the reasons discussed below, and based on the record before us, we determine that Petitioner does not demonstrate a reasonable likelihood of prevailing in showing that the independent claims would have been obvious.

In Templin, the content creator or sender provides data indicating how the system is to authenticate viewers. Ex. 1005, 3:26–34. Templin describes several ways to authenticate viewers; two ways are most relevant to the case at hand. *See id.* at 3:53–58 (listing various authentication methods), 3:59–4:25 (providing further detail of each).

In the first method, the creator provides an email address of an authorized viewer. *Id.* at 4:16–22. When a content viewer goes to access the content, the system sends an access code to the email address on file. *Id.*

If the content viewer has access to that email account, they would then see the code in their email, and be able to proceed. *See id.*

The second method uses a third-party authentication provider. Ex. 1005, 4:3–15. In this method, a web server storing a resource that the viewer wants to access (e.g., web server 114 in Figure 1) presents the viewer with the authentication interface of a third-party authentication provider. *Id.* at 4:6–9, 7:49–53. For example, the web server would present the viewer with an interface prompting the viewer to enter a Gmail address and password (if Gmail OpenID service is used as the third-party authentication service) or Twitter ID and password (if Twitter's oAuth service is used). *Id.* at 4:5–15. The third-party authentication service would then inform the web server if authentication succeeded or failed. *Id.* at 4:9–10. The server provides access to the content upon successful authentication of the user identity by the appropriate third-party authentication provider. *Id.* at 7:46–67.

As described earlier, the claimed method also uses third-party "identity providers," i.e., authentication providers. *See* Ex. 1011, 14:39–57 (providing an example using Gmail). First, the method verifies whether the user attempting to access the content has a user identifier included in the received information associated with the encrypted data object. *Id.* at 11:12–15, 22:23–26 ("verifying . . ."). Second, the method selects the identity provider that is implicated by that user identifier. *Id.* at 15:62–66, 22:26–31 ("selecting . . ."). Third, the method uses that identity provider to authenticate the user. *Id.* at 22:32–34 ("requesting . . . authentication"). Independent claim 4 contains the same recitations. *Id.* at 22:61–23:6.

Although both the claimed method and that disclosed in Templin describe using third-party authentication of a pre-authorized user identity, the dispositive issue in this case is whether the prior art shows an additional step of verifying that the user is identified in the received information associated with the encrypted data object, separate from third-party authentication of the user.

Petitioner maps the verifying step to the email-code method of authorization in Templin (Pet. 18–19) and the requesting authentication step to the use of a third-party authentication provider in Templin (*id.* at 31–32). Thus, Petitioner's analysis requires the use of both the email-code and third-party authentication methods.

Patent Owner responds that "Templin does not teach an embodiment where email authentication and third-party system authentication co-exist"; that is, "Templin does not disclose performing an initial authentication (*e.g.*, email authentication) and a second subsequent authentication (*e.g.*, third-party system authentication) as required by Petitioner's mapping" of the verifying and requesting authentication limitations. Prelim. Resp. 39–40. Patent Owner further asserts that Petitioner "fails to provide a motivation to combine these two embodiments of Templin" and one of ordinary skill in the art "would not have been motivated to combine the email authentication and third-party system authentication embodiments of Templin." *Id.* at 39, 41. According to Patent Owner, combining the embodiments would be contrary to Templin's goal of reducing the amount of unnecessary information shared with the web server and would be contrary to Petitioner's proffered reason to combine the teachings of Templin and McDaniel. *Id.* at 41–43.

We agree with Patent Owner. Petitioner does not identify where Templin discloses using email authentication and third-party authentication in serial fashion. Nor does Petitioner explain why it would have been obvious to use both mechanisms in the process of validating one user, and obviousness cannot be shown merely by pointing to disparate features of a disclosure. *KSR*, 550 U.S. at 418 ("[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.").

Petitioner takes another approach, asserting that it would have been obvious to verify whether the user is identified in the received information associated with the encrypted data object, prior to using the third-party verification feature of Templin. Pet. 18–19. Petitioner asserts that it would have been obvious to do so because "it would be inefficient to attempt to authenticate a viewer that was not previously verified to be among those approved to view the message." *Id.* at 19. We do not credit this attorney argument, for which Petitioner does not provide sufficient factual support or technical reasoning. *See, e.g.*, *Estee Lauder Inc. v. L'Oreal, S.A.*, 129 F.3d 588, 595 (Fed. Cir. 1997) ("arguments of counsel cannot take the place of evidence lacking in the record" (citation omitted)). Further, it is not clear why Petitioner's proposed modification would be more efficient, given that Templin's system already avoids authenticating viewers not previously authorized to view the message: web server 114 would only authenticate a viewer that first presents a hashed cryptographic asset that matches a hashed cryptographic asset previously stored with the web server. Ex. 1005, 7:1–9, 7:46–53. Because the hashed asset presented by the viewer and the hashed asset stored by the web server both originate from the creator (*id.* at 7:1–4),

only viewers authorized by the creator would be authenticated. Petitioner would seemingly propose that the system: (1) obtains a user name, (2) checks whether the user is identified in information previously received from the creator, and then (3) proceeds to the third-party authentication of the user. As it stands, the relevant embodiments in Templin simply require email-code authentication or third-party authentication. Ex. 1005, 7:46–60; *see also* Prelim. Resp. 55 (arguing that "Petitioner's alleged combination would require that the modified system perform *two* separate authentication steps instead of one"). Thus, Petitioner's argument that it would have been obvious to *add* a step (not disclosed in the prior art) in order to be more efficient is not persuasive on this record.

Petitioner also asserts that verifying whether the user is identified in the received information associated with the encrypted data object furthers Templin's stated goal of preventing unauthorized users from accessing the content. Pet. 19 (citing Ex. 1005, 6:39–45). But this would appear to be what Templin's third-party authentication already does; it uses a third party to determine if a user is authorized (that is, not unauthorized). Ex. 1005, 6:39–45; *see also* Prelim. Resp. 55 (arguing that "Templin already discloses that its system prevents third-party interceptors from accessing encrypted content"). Petitioner has not shown where Templin suggests a separate verification step prior to authentication, nor explained sufficiently why the goal in Templin of "preventing unauthorized access" would lead a person of ordinary skill in the art to add a new, undisclosed verifying step to Templin's existing authorization scheme.

Lastly, Petitioner asserts that McDaniel discloses the user-verification limitation. Pet. 19–24. Petitioner relies on a portion of the process shown in

Figure 4 of McDaniel, in which a user operating client 108 requests access to a resource service provided by resource server 114. *Id.* at 19–20 (citing Ex. 1007, 8:24–34, 10:43–57, 11:10–24, 14:29–61, Fig. 4. According to the excerpt of McDaniel quoted by Petitioner, if resource server 114 determines that the user must be authenticated before being granted access to the service, the server prompts the user to provide user credentials, such as a user name and password; once the user name and password are supplied, web server 114 determines whether "the user name is valid and the password is correct." Ex. 1007, 14:43–59; *see also* Pet. 21–22 (quoting same). Petitioner asserts that "[a] POSITA would understand McDaniel to disclose a resource server that verifies a user of a client device ('second user') is identified in stored authentication information (stored information against which the client's credential information is checked), and that the resource server does so in the context of authenticating the user for access to a protected resource." Pet. 22 (citing Rosenblatt ¶¶ 81–84). Petitioner further asserts that one of ordinary skill in the art would have been motivated "to incorporate these teachings from McDaniel into Templin, such that Templin's server verifies that a user is identified in information 112" because the combination amounts to "the use of a known technique (McDaniel's authentication techniques, involving verification of user identifier information) to improve a similar system (Templin's encryption system) in the same way contemplated by McDaniel—to verify a user's identity before allowing the user to access a particular protected resource." *Id.* at 22–23.

Patent Owner notes that the Petition maps McDaniel's user credentials provided by a user seeking access to content during basic authentication to

the recited verifying step (Prelim. Resp. 48 (citing Pet. 22[3])) and argues that McDaniel does not disclose verifying that such user credentials are in received information associated with an encrypted data object (*id.* at 49). Patent Owner further asserts that one of ordinary skill in the art would not have been motivated to combine McDaniel's basic authentication process, which requires the resource server to manage and receive "sensitive user data" (the username and password) because it would conflict with Templin's goal of authenticating a viewer without the web server "being privy to any sensitive data from those [third-party authentication] services." *Id.* at 52 (alteration in original) (citing Ex. 1005, 4:10–13).

McDaniel describes a system to provide authentication. Ex. 1007, code (54). The user of a client device provides a username and password to a resource server, which, according to Petitioner, verifies whether the user is identified in information stored at the resource server. Pet. 22 (citing Ex. 1002 ¶¶ 81–84).

We are not persuaded that one of ordinary skill in the art would have combined Templin and McDaniel to arrive at both the claimed user-verification step and authentication-request step. Even assuming Petitioner is correct in its assertion that McDaniel in some sense "verifies" a user of a client device when the user successfully presents a user name and password (Pet. 22), Templin already discloses an embodiment where the system authenticates the user by a third-party identity server interface (e.g., by successfully providing a user name and password) (Ex. 1005, 4:7:46–60; *see*

[3] Throughout its Preliminary Response, Patent Owner consistently mistakenly refers to the Petition as Paper 1 rather than Paper 2. We treat these mistakes as harmless errors.

also Ex. 1023, 1 ("Websites that accept OpenID can now [use Gmail to] sign in . . . ."). Petitioner does not direct our attention to where McDaniel teaches or suggests the *separate* verifying and selecting steps recited in the claims.

Additionally, Petitioner has not persuaded us that McDaniel's "stored authentication information" that Petitioner asserts would be used to perform basic authentication corresponds to the claimed "received information associated with the encrypted data object" that is received "from a first client device." Further, if one of ordinary skill in the art were to combine the teachings of Templin and McDaniel, it would seem more likely that McDaniel's basic authentication would be used as an alternative to Templin's third-party authentication, just as Templin teaches that email authentication and other authentication methods are alternatives to third-party authentication. *See* Ex. 1005, 3:53–58. To the extent Petitioner's ground here implies that it would have been obvious to perform two authentication steps, one serving as the claimed verification step and one serving as the claimed selecting/authentication steps, Petitioner has not persuaded us why one of ordinary skill in the art would have done so. *Panduit Corp. v. Dennison Mfg. Co.*, 774 F.2d 1082, 1092 n.16 (Fed. Cir. 1985) ("The question, however, is never whether an invention *could* be made, but whether there is anything in the prior art as a whole that would have rendered its making obvious to one skilled in the art when the invention was made"), *vacated and remanded on other grounds*, *Dennison Mfg. Co. v. Panduit Corp.*, 475 U.S. 809 (1986).

For at least these reasons, we agree with Patent Owner that Petitioner has not established a reasonable likelihood of success in showing that claim 1 is unpatentable. Petitioner has the same deficiency in its showings

for independent claim 4 (Pet. 48). We do not address further the challenged dependent claims because Petitioner has not made sufficient showings for their respective independent claim, and Petitioner does not bring in additional references that would cure the above-noted deficiencies.[4]

IV. CONCLUSION

For the foregoing reasons, we are not persuaded that the Petition establishes a reasonable likelihood that Petitioner would prevail in any of its challenges to claims 1–5 of the '021 patent.

V. ORDER

In consideration of the foregoing, it is hereby ordered that the Petition is *denied*, and no trial is instituted.

[4] Petitioner relies on Gilliam to teach a data rights protection mechanism as recited in claim 4 (*see* Pet. 44–50) but does not rely on Gilliam in any manner that addresses the shortcomings noted above.

For PETITIONER:

Christina J. McCullough
Samantha Hunt
PERKINS COIE LLP
mccullough-ptab@perkinscoie.com
hunt-ptab@perkinscoie.com

For PATENT OWNER:

Mehran Arjomand
Alex S. Yap
Fahd H. Patel
Joshua A. Crawford
Anya P. Adams
MORRISON & FOERSTER LLP
marjomand@mofo.com
ayap@mofo.com
fpatel@mofo.com
jcrawford@mofo.com
aadams@mofo.com