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.

IPR2023-00017
Patent 8,589,673 B2

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

SAINDON, *Administrative Patent Judge.*

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

I. INTRODUCTION

A. Background and Summary

Microsoft Corporation ("Petitioner") filed a Petition (Paper 2, "Pet.") requesting *inter partes* review of claims 1, 5–9, and 11–19 ("the challenged claims") of U.S. Patent 8,589,673 B2 (Ex. 1001, "the '673 patent"). Pet. 2. Virtru Corporation ("Patent Owner") filed a Preliminary Response (Paper 8, "Prelim. Resp.").

We have authority to determine whether to institute an *inter partes* review under 35 U.S.C. § 314(b) and 37 C.F.R. § 42.4(a). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted unless "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition."

For the reasons provided below, we determine Petitioner has not satisfied the threshold requirement set forth in 35 U.S.C. § 314(a). Because Petitioner has not demonstrated a reasonable likelihood that at least one claim of the '673 patent is unpatentable, we do not institute an *inter partes* review.

Our findings of fact, conclusions of law, and reasoning discussed below are based on a preliminary evidentiary record, and made for the purpose of determining whether the Petition meets the threshold for initiating review. This decision not to institute trial is not a final decision as to the patentability of any challenged claim.

B. Real Parties in Interest

The parties do not identify any further real parties in interest. Pet. 1; Paper 5, 1 (Patent Owner's Mandatory Notices).

C. Related Matters

The parties identify *Virtru Corporation v. Microsoft Corporation*, 6-22-cv-00242 (WDTX) as a matter in which the '673 patent has been asserted against Petitioner. Pet. 1; Paper 5, 1. Petitioner has also filed petitions challenging Patent Owner's patents US 8,874,902 in IPR2023-00018 and US 9,578,021 in IPR2023-00019. Pet. 1.

D. Prior Art and Asserted Grounds

Petitioner's grounds rely on the following prior art references:

Name	**Reference**	**Exhibit(s)**
Templin	US Pat. 8,898,482 B2, iss. Nov. 25, 2014	1005
McDaniel	US Pat. 9,736,153 B2, iss. Aug. 15, 2017	1007

Petitioner asserts that claims 1, 5–9, and 11–19 would have been unpatentable on the following grounds:

Claim(s) Challenged	**35 U.S.C. §**[1]	**Reference(s)/Basis**
1, 5–9, 11–19	103	Templin
1, 5–9, 11–19	103	Templin, McDaniel

E. Overview of the '673 Patent

The '673 patent states that it is directed to a method and system for distributing cryptographic data to authenticated recipients. Ex. 1001, code (54). In example embodiments, information is associated with an encrypted data object, such as the encryption key used to encrypt the data object and an

[1] The '673 patent was filed on December 30, 2011 and claims priority to a provisional application filed January 12, 2011. Ex. 1001, codes (22), (60). We apply the versions of 35 U.S.C. §§ 102 and 103 that were in force before they were amended by the Leahy-Smith America Invents Act, Pub. L. No. 112–29, 125 Stat. 284 (2011).

access control list that specifies which users may receive the encryption key. *Id.* at 8:35–46. The system uses a third-party authentication provider to authenticate users. *See id.* at 9:61–10:26. In practice, the system first verifies whether a user seeking access to an encrypted object is listed on the access control list. *Id.* at 10:27–30, 14:1–6. Then, the system identifies the third-party authentication provider implicated by the user identifier. *Id.* at 12:46–53. Having identified the provider, the system lastly requests that the provider authenticate the user. *Id.* at 12:46–63. Figure 3 of the '673 patent, reproduced below, depicts a flowchart of these steps:

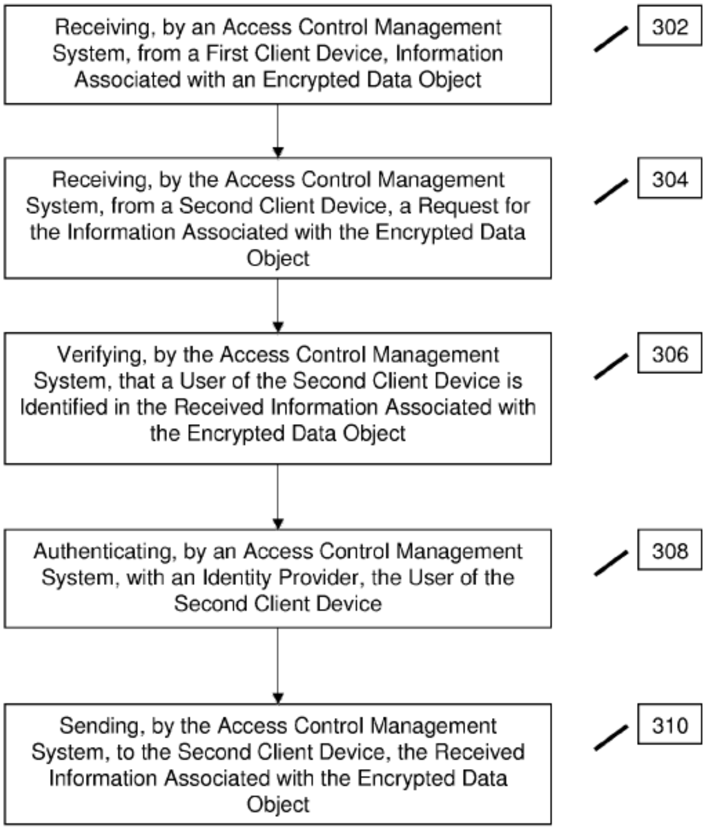
Receiving, by an Access Control Management System, from a First Client Device, Information Associated with an Encrypted Data Object
302
Receiving, by the Access Control Management System, from a Second Client Device, a Request for the Information Associated with the Encrypted Data Object
304
Verifying, 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
306
Authenticating, by an Access Control Management System, with an Identity Provider, the User of the Second Client Device
308
Sending, by the Access Control Management System, to the Second Client Device, the Received Information Associated with the Encrypted Data Object
310

Fig. 3

Ex. 1001, Fig. 3. Figure 3 of the '673 patent depicts a flowchart listing the steps just described.

F. Challenged Claims

Claims 1, 5–9, and 11–19 are challenged. Claims 1, 18, and 19 are independent. Claim 1 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; and
>
> 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;
>
> receiving, by an access control management system, from the first client device, information associated with a second encrypted data object;
>
> receiving, by the access control management system, from a third client device, a request for the information associated with the second encrypted data object;
>
> verifying, by the access control management system, that a user of the third client device is identified in the received information associated with the second encrypted data object;

> automatically selecting, by the access control management system, a second identity provider from the plurality of identity providers, based on a second user identifier included in the received information associated with the encrypted data object, the second user identifier associated with the user of the third client device;
>
> automatically requesting, by the access control management system, from the selected second identity provider, authentication of the user of the third client device; and
>
> sending, to the third client device, the received information associated with the second encrypted data object, responsive to the authentication of the user of the second client device by the second identity provider.

II. ANALYSIS

A. Legal Standards Used in the Merits Analysis

"In an IPR, 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")); *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review).

A claim is unpatentable under 35 U.S.C. § 103 if "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 . . . to a person having ordinary skill in the art to which said 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, objective evidence of nonobviousness, i.e., secondary considerations. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Petitioner asserts that a person of ordinary skill in the art:

> 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. More education can supplement practical experience and vice versa.

Pet. 3 (internal citations removed).

Patent Owner does not appear to comment on the level of ordinary skill in the art. We adopt Petitioner's definition for purposes of this Decision.

C. Claim Construction

Neither party proposes a claim construction. Pet. 7 ("Petitioner does not contend that formal construction of any claim term is necessary."); Prelim. Resp. 15–16 ("Patent Owner submits that the Board need not construe any claim terms for the purpose of this proceeding."). We discern no claim construction to be necessary for us to reach our decision. Accordingly, we construe no terms. *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

D. Asserted Obviousness in View of Templin and McDaniel

Petitioner asserts that the method of claim 1 is obvious in view of Templin, or in view of Templin and McDaniel. Pet. 8–39. Petitioner applies the same analysis to independent claims 18 and 19 (*id.* at 49–61), which are similar in scope but recite a computer readable medium and a system, respectively.

In Templin, the content creator or sender provides information to an encryption system sufficient to ensure that prospective content viewers are authorized to access the sender's encrypted content. Ex. 1005, 3:26–35. For example, the content creator can provide data indicating how the system is to authenticate viewers. *Id.* Templin describes several ways to do this; 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).

The first method uses an email code. 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 use the code to proceed. *See id.*

The second method uses a third-party authentication provider. *Id.* at 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's 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. Templin discloses that it would provide access to the content upon successful authentication of the user identity by the appropriate third-party authentication provider. *Id.* at 7:47–67.

As described earlier, the claimed system also uses third-party "identity providers," i.e., authentication providers. *See* Ex. 1001, 13:49–67 (providing an example using Gmail). First, the method verifies whether the user attempting to access the content has a user identifier listed in the list of authorized users. *Id.* at 10:27–30, 21:20–23 ("verifying . . .").[2] Second, the method selects the identity provider that is implicated by that user identifier. *Id.* at 15:3–7, 21:24–29 ("selecting . . ."). The third step is to use that identity provider to authenticate the user. *Id.* at 21:30–33 ("requesting . . . authentication").

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 on the list of authorized users, separate from referring the user to the third-party authentication provider.

Petitioner maps the verifying step to the email-code method of authorization in Templin (Pet. 17–18) and the requesting authentication step to the use of a third-party authentication provider in Templin (*id.* at 30–31).

[2] For simplicity, we use the term "list of authorized users," but note that the claim language more broadly states "information associated with the encrypted data." The specification provides an access control list as an example. Ex. 1001, 10:26–37.

Thus, Petitioner's analysis requires the use of both the email-code and third-party authentication methods.

Patent Owner argues that Templin's email-code method, however, is its own independent verification mechanism, separate from the verification mechanism using a third-party authentication provider. Prelim. Resp. 38–43. We agree with Patent Owner. Petitioner does not identify where Templin discloses using the email-code authentication and third-party authentication mechanisms 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 on the list of authorized users, prior to using the third-party verification feature of Templin. Pet. 17–18. Petitioner asserts that it would have been obvious to do so because "it would be inefficient to attempt to verify a viewer that was not among those approved to view the message." *Id.* at 18. 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") (internal citations and quotation marks omitted). Further, it is not clear why Petitioner's proposed modification would be more efficient. Petitioner would seemingly propose that the system: (1) obtains a user name, (2) checks whether the user is on the list, and then

(3) proceeds to the third-party authentication of the user. As it stands, the relevant embodiments in Templin simply require email-code or third-party authentication. Ex. 1005, 7:46–60; *see also* Prelim. Resp. 54 (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 in order to be more efficient is not persuasive on this record.

Petitioner also asserts that verifying whether the user is on the list of authorized users furthers Templin's stated goal of preventing unauthorized users from accessing the content. Pet. 18 (citing Ex. 1005, 6:39–45). But this would appear to be what Templin's third-party authentication embodiment already does; it uses a third party to determine if a user is authorized. Ex. 1005, 6:39–45; *see also* Prelim. Resp. 54 (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 suggests adding the claimed verification step to Templin. Pet. 19–23. Patent Owner disputes that assertion. *See generally* Prelim. Resp. 43–55.

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 are checked with an identity server to determine whether to authenticate the user. *Id.* at 7:46–64. The resource server acts as a proxy for the identity server in situations where, due to technical limitations, the client device cannot interact directly with the identity server. *Id.* at 1:26–40, 3:15–42.

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. 21), 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, 4:3–15, 7:46–60; *see also* Ex. 1023, 1 ("Websites that accept OpenID can now [use Gmail to] *sign in* . . . .") (emphasis added)). Petitioner does not direct our attention to where McDaniel teaches or suggests the *separate* verifying and selecting steps recited in the claims. To the extent Petitioner's ground here implies that it would have been obvious to effectively provide a user name and password login twice, first serving as the claimed verification step and then serving as the claimed selecting/authentication steps, Petitioner has not explained how we should interpret the claims in such a manner or why it would have been obvious to do 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 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 claims 18 (Pet. 51–52) and 19 (*id.* at 58). 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.

III. CONCLUSION

Petitioner has not established a reasonable likelihood of success in showing that any claim is unpatentable over Templin or Templin and McDaniel. We do not institute an *inter partes* review.

IV. ORDER

In consideration of the foregoing, it is hereby ORDERED that *inter partes* review of claims 1, 5–9 and 11–19 of the ’673 patent is denied.

FOR PETITIONER:

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

FOR PATENT OWNER:

Mehran Arjomand
Alex Yap
Fahd Patel
Joshua Crawford
Anya Adams
MORRISON FOERSTER
marjomand@mofo.com
ayap@mofo.com
fpatel@mofo.com
jcrawford@mofo.com
aadams@mofo.com