UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/693,479	12/04/2012	Simon Gilbert Canning	AU920120018US1	2824

63400 7590 06/29/2020

IBM CORP. (DHJ)
c/o DAVID H. JUDSON
5960 Berkshire Ln, Floor 6
SUITE 225
DALLAS, TX 75225

EXAMINER	
THIAW, CATHERINE B	

ART UNIT	PAPER NUMBER
2493	

NOTIFICATION DATE	DELIVERY MODE
06/29/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mail@davidjudson.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SIMON GILBERT CANNING, DAVID PAUL MOORE,
SHANE BRADLEY WEEDEN, and STEPHEN VISELLI

Appeal 2019-002646
Application 13/693,479
Technology Center 2400

Before JASON J. CHUNG, BETH Z. SHAW, and
JASON M. REPKO, *Administrative Patent Judges*.

REPKO, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Under 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1–22 and 25–28. Claims 23 and 24 are canceled. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42(a). According to Appellant, the real party in interest is International Business Machines Corporation. Appeal Br. 1.

CLAIMED SUBJECT MATTER

Appellant's invention relates to a policy-based approach to securing enterprise data on mobile devices. Spec. 1:5–6. The invention addresses issues related to bring-your-own-device (BYOD) in the workplace—i.e., employees own their devices but use them to run enterprise applications. *Id.* at 1:17–19. Under BYOD, enterprises must ensure that a user's personal device does not leak sensitive enterprise data. *Id.* at 1:20–21. BYOD poses other security risks associated with lost or stolen devices, confidential-information management, and unauthorized access to the corporate network. *Id.* at 1:21–23.

Appellant's invention seeks to balance information-security requirements with the device's usability. *Id.* at 3:4–7. To this end, the invention creates a risk profile for each device. *Id.* at 4:2–4. The risk profile is based on the device's installed applications, the user's services, and the operations that the user has authorized the device to perform. *Id.* at 4:2–5. One embodiment uses an authorization server to track an application's "authorization scope." *Id.* at 4:11–12. The system enforces a security policy when the applications are used. *Id.* at 4:16–18. According to the Specification, this approach maintains the device's usability without compromising enterprise security. *Id.* at 4:18–20.

Claims 1, 8, 15, and 22 are independent. Claim 1 is reproduced below.

> 1. A method to enforce an enterprise security policy when a request for access to a service of the enterprise is initiated at a mobile device having a security policy enforcement agent and at least one personal application, comprising:
>
> responsive to authentication of a user that delegates from the user to the mobile device an authorization to access the service according to a scope of operations defined by the user of the mobile device and by which the

> user is permitted to delegate to the mobile device that authorization, providing a notification to the mobile device security policy enforcement agent that a security policy associated with the mobile device has changed as a result of the delegation, the changed security policy requiring at least one additional security constraint as determined by the enterprise security policy and being based in part on the user-defined scope of operations;
>
> responsive to receiving a notification from the mobile device security policy enforcement agent that the additional security constraint that is based in part on the user-defined scope of operations has been met at the mobile device, providing an authorization token to the mobile device;
>
> responsive to a subsequent receipt of the authorization token from the mobile device together with a request that encapsulates information identifying what security policy is in use for this access, determining whether the authorization token is valid and whether the changed security policy is in force at the mobile device; and
>
> responsive to a determination that the authorization token is valid and that the changed security policy is in force at the mobile device, permitting access to the service.

Appeal Br. 27 (Claims Appendix).[2]

[2] Throughout this opinion, we refer to the Final Office Action ("Final"), mailed May 31, 2018; the Advisory Action ("Advisory"), mailed September 18, 2018; the Appeal Brief ("Appeal Br."), filed October 31, 2018; the Examiner's Answer ("Ans."), mailed December 21, 2018; and Reply Brief ("Reply Br."), filed February 15, 2019.

REFERENCES

The Examiner relies on the references in the table below.

Name	Reference	Date
Herrmann	US 2004/0167984 A1	Aug. 26, 2004
Nguyen	US 2008/0028453 A1	Jan. 31, 2008
Srinivasan	US 2013/0086645 A1	Apr. 4, 2013
Hendrickson	US 2013/0162753 A1	June 27, 2013
Qureshi	US 2014/0007222 A1	Jan. 2, 2014

REJECTIONS

The Examiner rejects claims 1–4, 8–11, 15–18, 22, and 25–28 under 35 U.S.C. § 103 as unpatentable over Herrmann, Hendrickson, and Qureshi. Final 9–18.

The Examiner rejects claims 5, 12, and 19 under 35 U.S.C. § 103 as unpatentable over Herrmann, Hendrickson, Qureshi, and Srinivasan. Final 18.

The Examiner rejects claims 6, 7, 13, 14, 20, and 21 under 35 U.S.C. § 103 as unpatentable over Herrmann, Hendrickson, Qureshi, and Nguyen. Final 19–20.

OPINION

The Rejection over Herrmann, Hendrickson, and Qureshi

In the rejection of claim 1, the Examiner finds that Herrmann teaches all limitations except for (1) the user-defined scope of operations and (2) the recited agent. *See* Final 9–12. Specifically, the Examiner finds that Herrmann teaches accessing the service according to the scope of operations defined by an administrator, but Hendrickson teaches a scope of operations from a user. *See* Ans. 5. The Examiner finds that Hendrickson's configuration of a video conference corresponds to the recited user-defined scope of operations. Final 11; Ans. 5.

Appellant's Arguments

According to Appellant, "The notion of the user delegating something to the mobile device itself is neither disclosed nor suggested" by Hendrickson. Appeal Br. 17. In Appellant's view, Hendrickson's server simply authorizes a user to connect to a video conference. *Id.* at 16. Appellant also argues that Qureshi's agent does not enforce a security policy that has changed as a result of a delegation. *Id.* at 19.

Issue

Under § 103, has the Examiner erred in finding that Herrmann, Hendrickson, and Qureshi collectively teach or suggest a user that delegates from the user to the mobile device an authorization to access the service according to a scope of operations and a security policy that has changed as a result of this delegation, as required by claim 1?

Analysis

Claim 1 recites, in part,

> a user that *delegates* from the user to the mobile device an authorization to access the service according to a scope of operations defined by the user of the mobile device and by which the user is permitted to *delegate* to the mobile device that authorization;

Appeal Br. 27 (Claims Appendix) (emphases added). Claim 1 further requires a "security policy associated with the mobile device has changed as a result of the delegation." *Id.*

The Examiner interprets a delegation as encompassing a user accessing the service:

> The user through his device being granted access to the service (or being delegated), then accesses the service according to a scope of operations allowed ([0074]) meaning the user accesses the requested service as a response to being authenticated according to a scope of operations by which the user is permitted to delegate to the mobile device (user device) that authorization.

Ans. 5. In the Examiner's view, "any setting performed by a user to authorize his device to access a service teaches a user delegating his device to access a service (which the device cannot do alone)." Final 2. The Examiner finds that there is a delegation "each time a user sets his device to access the service." Ans. 9. We agree with Appellant that the Examiner's interpretation of delegation is unreasonably broad because it reads out claim limitations and is inconsistent with the Specification. *See* Appeal Br. 11–13, 16–17.

During examination, claims are to be given their broadest reasonable interpretation. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). When applying the broadest reasonable interpretation, examiners read the claim in light of the specification as it would be interpreted by one of ordinary skill in the art. *Id.* But the broadest *reasonable* interpretation is not the broadest *possible* interpretation. *In re Smith Int'l, Inc.*, 871 F.3d 1375, 1383 (Fed. Cir. 2017). Rather, the interpretation must be "consistent with the specification." *Id.* at 1382–83 (quoting *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997)). Limitations, though, must not be read into the claims from the specification. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

Here, claim 1 requires that the delegation must be "from the user to the mobile device." The Specification consistently uses the term "delegate" to mean grant. *See, e.g.*, Spec. 19:5–9. For instance, the Specification explains that "if the user chooses to grant (delegate) authorization," the server notifies the mobile device's security-policy enforcement agent. *Id.* In other words, the user is the grantor, and the mobile device is the grantee.

Also, the delegation is not immediately "actionable," as Appellant argues. Appeal Br. 17. Rather, the delegation results in the mobile device enforcing the security constraints in the policy.

By contrast, in the Examiner-cited embodiment, Herrmann's user simply accesses a server with a device. Ans. 3 (citing Herrmann ¶¶ 72, 74). Specifically, a user, Alice, is normally granted all privileges to a file stored on a server when she is on her office computer at work. Herrmann ¶ 74. But when Alice connects to the server from her home computer, the system reduces Alice's access privileges if the system determines that her computer does not comply with the security policy. *Id.*

The Examiner has not shown that Alice delegates anything to the mobile device here. Rather, Herrmann teaches that Alice simply connects to the server using a home or office computer, and the system grants or denies access. *Id.* Thus, we agree with Appellant that the Examiner has not shown that Herrmann teaches that the user delegates or is permitted to delegate to the user's device the recited authorization. *See* Appeal Br. 12–13.

We also agree with Appellant that Hendrickson does not cure Herrmann's deficiencies in this regard. *Id.* at 16–17. Hendrickson generally relates to configuring a video conference. Hendrickson ¶ 55. Hendrickson's user provides setup information to the server. *Id.* The setup information specifies the user's account (e.g., username, password, and personal identification number), the user's device (e.g., device identifier, IP address, and MAC address), and a conference to be held (e.g., start time, end time, and expected duration). *Id.* ¶ 56. Hendrickson's authorization process uses a server, VCCS 130, to authorize access. *See, e.g.*, *id.* ¶ 58. For example, VCCS 130 checks whether client device 110 is permitted to access the conference. *See id.* ¶¶ 55–56, 58, 68, 77–78.

According to the Examiner, Hendrickson's user makes the recited delegation when the user enters the conference settings. Ans. 6 (citing Hendrickson ¶¶ 55–56, 58, 68, 77–78). Hendrickson's user, though, simply manages how the server permits a user's client to access the videoconference that the server executes, as Appellant argues. Appeal Br. 17. In claim 1, after the user makes the recited delegation, it is the user's device that requires additional security constraints to be enforced before the device is permitted to access the service. *Id.*

In analyzing Herrmann and Hendrickson, the Examiner interprets delegating as permitting access. *See* Ans. 5 ("being granted access to the service (or being delegated)"); Final 2 (explaining that a user "authoriz[ing] his device to access a service teaches a user delegating"). But the method of claim 1 does not permit access until after other conditions are met. That is, claim 1 recites "responsive to a determination that the authorization token is valid and that the changed security policy is in force at the mobile device, *permitting access to the service*." Appeal Br. 27 (Claims Appendix) (emphasis added).

Thus, the Examiner has erred in finding that Hendrickson, Herrmann, or some combination of these references teach or suggest a changed security policy where the user delegates to the mobile device an authorization to access the service according to the recited limitations.

The Examiner also cites Qureshi for the limited purpose of teaching an agent installed on a client mobile device. Final 11 (citing Qureshi ¶¶ 83, 245, 258). The Examiner, though, does not find that Qureshi teaches or suggests any affirmative delegation to that mobile device, as recited. *See id.*; *see also* Ans. 9 (discussing Qureshi).

On this record, we do not sustain the rejection of claim 1. We also do not sustain the rejection of independent claims 8, 15, and 22, which recite similar limitations, and dependent claims 2–4, 9–11, 16–18, and 25–28, for similar reasons.

The Rejection over Herrmann, Hendrickson, Qureshi, and Srinivasan

In rejecting claims 5, 12, and 19, the Examiner cites Srinivasan for the limited purpose of showing that the recited token revocation was known. Final 18. Because the Examiner has not shown that Srinivasan cures the above-noted deficiencies, we also do not sustain the obviousness rejection of claims 5, 12, and 19.

The Rejection over Herrmann, Hendrickson, Qureshi, and Nguyen

In rejecting claims 6, 7, 13, 14, 20, and 21, the Examiner cites Nguyen for the limited purpose of showing that the recited mapping was known. Final 19–20. Because the Examiner has not shown that Nguyen cures the above-noted deficiencies, we also do not sustain the obviousness rejection of claims 6, 7, 13, 14, 20, and 21.

CONCLUSION

We reverse the Examiner’s rejection of claims 1–22 and 25–28.

DECISION SUMMARY

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–4, 8–11, 15–18, 22, 25–28	103	Herrmann, Hendrickson, Qureshi		1–4, 8–11, 15–18, 22, 25–28
5, 12, 19	103	Herrmann, Hendrickson, Qureshi, Srinivasan		5, 12, 19
6, 7, 13, 14, 20, 21	103	Herrmann, Hendrickson, Qureshi, Nguyen		6, 7, 13, 14, 20, 21
Overall Outcome				1–22, 25–28

REVERSED