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.
12/268,053	11/10/2008	Michael J. CURRIER	END920080200US1	7452

46583 7590 06/02/2020
Roberts Calderon Safran & Cole, P.C.
Intellectual Property Department
P.O. Box 10064
MCLEAN, VA 22102-8064

EXAMINER	
BAHL, SANGEETA	

ART UNIT	PAPER NUMBER
3629	

NOTIFICATION DATE	DELIVERY MODE
06/02/2020	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):

docketing@rcsc-ip.com
lgallaugher@rcsc-ip.com
secretaries@rcsc-ip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MICHAEL J. CURRIER, DUANHUA TU,
SUNIL JOSHI, MURTHY V. RALLAPALLI,
and LISA N. SCHENKEWITZ

Appeal 2019-003253
Application 12/268,053
Technology Center 3600

Before ALLEN R. MACDONALD, ERIC B. CHEN, and
IFTIKHAR AHMED, *Administrative Patent Judges.*

AHMED, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants[1] appeal under 35 U.S.C. § 134(a) from the Examiner's decision rejecting claims 1–27, which are all of the claims pending in the application. 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). Appellant identifies International Business Machines Corporation as the real party in interest. Appeal Br. 2.

TECHNOLOGY

The claims relate to "enterprise privacy information compliance (EPIC) and, in particular, to scanning and interrogating a site for privacy compliance based on one or more privacy standards." Spec. ¶ 1.

ILLUSTRATIVE CLAIM

Claim 1 is illustrative and reproduced below with the limitations at issue emphasized:

> 1. A computer implemented method for determining privacy compliance comprising:
>
> automatically scanning, using an enterprise privacy compliance (EPIC) tool, one or more websites that have one or more privacy requirements with a web based tool using only server side code to automatically verify compliance with the one or more privacy requirements by ensuring that required privacy practices are in place on the one or more websites, wherein the one or more privacy requirements include a backout statement;
>
> the method further comprising:
>
> identifying, by the scanning and using the EPIC tool, at least one website associated with a uniform resource locator (URL);
>
> determining, by a processor and using the EPIC tool, whether the at least one website is compliant with the one or more privacy requirements, wherein the determining includes *analyzing configuration details of a server by restricting encryption ciphers that the server is capable of using*;
>
> generating, by the EPIC tool, a report indicating which of the one or more privacy requirements are met and which of the one or more privacy requirements are unmet based on the determining; and
>
> outputting, by the EPIC tool, the report, wherein the report provides immediate feedback on whether the at

> least one website is compliant, and guidance on modifying the at least one website to meet the one or more privacy requirements to reduce a probability that the at least one website will fail compliance.

REFERENCES

The Examiner relies upon the following prior art references:

Mulligan	US 7,467,107 B1	Dec. 16, 2008
Epling	US 2005/0091101 A1	Apr. 28, 2005
Clayton	US 2005/0149452 A1	July 7, 2005
Currie	US 2005/0160286 A1	July 21, 2005
Johnson	US 2005/0187891 A1	Aug. 25, 2005
Conboy	US 2005/0262063 A1	Nov. 24, 2005
Pueblas	US 2007/0199064 A1	Aug. 23, 2007
Edwards	US 2008/0133500 A1	June 5, 2008
Stollman	US 2010/0074524 A1	Mar. 25, 2010
Clayton	US 2005/0091101 A1	Apr. 28, 2005
Svantesson	Svantesson, *Geo-location technologies and other means of placing borders on the borderless' Internet*, available at http:// epublications.bond.edu.au/ law_pubs/63	Sept. 1, 2004

REJECTIONS

Claims 1, 4–6, 8–10, and 12–15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Conboy, Johnson, and Edwards. Final Act. 9.

Claims 2 and 3 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Conboy, Johnson, Edwards, and Clayton. Final Act. 20.

Claim 11 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Conboy, Johnson, Edwards, and Pueblas. Final Act. 22.

Claims 17–24 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Conboy, Johnson, Edwards, and Svantesson. Final Act. 23.

Claim 25 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Conboy, Johnson, Edwards, and Currie. Final Act. 30.

Claim 26 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Conboy, Johnson, Edwards, and Stollman. Final Act. 34.

Claim 27 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Conboy, Johnson, Edwards, Stollman, and Epling. Final Act. 34, 35.

ISSUE

Did the Examiner err in finding that Conboy teaches or suggests "analyzing configuration details of a server by restricting encryption ciphers that the server is capable of using," as recited in claim 1?

ANALYSIS

Independent claim 1 recites "analyzing configuration details of a server by restricting encryption ciphers that the server is capable of using." Appeal Br. 61 (Claims App.). Independent claims 8, 17 and 25 recite an identical limitation. The Examiner finds that Conboy teaches or suggests this limitation. Final Act. 11. According to the Examiner, Conboy teaches *extensible scan rules* that "use regular expressions, not unlike scripts and other high level language code, which define the search terms," and can also "incorporate logic tests and analysis." *Id.* (citing Conboy ¶ 27). The Examiner further finds that Conboy teaches that analysis parameters for these rules can include defining how the tested website's URLs are to be normalized, i.e., whether "[w]eb sites will direct users to servers in close geographic proximity, or use multiple servers which are load balanced." *Id.* (citing Conboy ¶ 97). The Examiner determines that this selection of servers corresponds to the disputed limitation because "[t]he examiner interprets 'restricting encryption ciphers' as algorithm restricting se[r]vers." *Id.* (citing Conboy ¶ 97).

Appellant argues that "there is no discussion of encryption ciphers in Conboy." Appeal Br. 43 (quoting Conboy ¶ 97). Appellant contends that Conboy's cited disclosure relates to "parameters for use in scanning tools in order to normalize URLs." *Id.* Appellant further disagrees the term "restricting encryption ciphers" can be interpreted as "an algorithm restricting servers." *Id.*

The Examiner counters by finding that the "[S]pecification is silent regarding *how* 'restricting encryption ciphers that the server is capable of using,'" is performed. Ans. 7. The Examiner further determines that the claimed method is not the only way in which privacy compliance may be determined, pointing out that the Specification discloses "inspect[ing] for privacy compliance by parsing text in the website, application, webpage, etc., for key words or features and comparing the parsed text against a database of privacy compliance verbiage and/or disclaimers." *Id.* (citing Spec. ¶ 44). Accordingly, the Examiner finds that Conboy's disclosure of parsing an XML document teaches or suggests the claim limitation. *Id.* at 6–7 (citing Conboy ¶¶ 98–100, 103, 105).

Moreover, the Examiner determines, Conboy discloses "tokenize data" which "effectively protect[s] data if implemented properly," and "essentially ha[s] the same function" as the claimed encryption algorithms. *Id.* (citing Conboy ¶¶ 83, 84, 428–432; Wikipedia, Tokenization, *available at* https://en.wikipedia.org/wiki/Tokenization_(data_security)).

As recited in claim 1, the "determining" step must include "analyzing configuration details of a server by restricting encryption ciphers that the server is capable of using" in order to determine "complian[ce] with one or more privacy requirements." Here, we agree with Appellant that the Examiner has not sufficiently explained how Conboy teaches or suggests analyzing configuration details of a server. *See* Appeal Br. 43–44; Reply Br. 16–19. Although we agree with the Examiner that the Specification discloses multiple embodiments for determining privacy compliance (Ans. 7), the claim recites *one* of those specific methods.[2]

Moreover, the Examiner misinterprets the claim limitation as an algorithm that restricts *the server to be used*. Rather, it is clear from the claim language that it is the *encryptions ciphers* that are restricted as the configuration of a given server is analyzed. Conboy's cited disclosure on the other hand relates to "normalizing URLs," writing Conboy's extensible scan rules in XML format, and preprocessing those XML documents prior to analysis of a website, none of which teaches or suggests actually analyzing configuration of a server or encryption ciphers. Conboy ¶¶ 98–105.

To the extent the Examiner is relying on string splitting operations disclosed in Conboy (¶¶ 83, 84, 428–432), those relate to the "functional programming capabilities" of Conboy's "XRules Language." *See, e.g.*, Conboy ¶ 72. It is not clear to us how that disclosure teaches or suggests analyzing configuration details either.

We, therefore, agree with Appellant that the Examiner has failed to explain sufficiently how Conboy teaches "analyzing configuration details of

[2] Although we agree with the Examiner's finding that the Specification fails to describe how the claimed "restricting encryption ciphers that the server is capable of using" is accomplished (Ans. 7), we do not address the Examiner's determination because the Examiner has not rejected any of the claims under 35 U.S.C. § 112, first paragraph. *See generally* Final Act.

a server by restricting encryption ciphers that the server is capable of using," as recited in claim 1. The Examiner also does not rely on Johnson and Edwards to teach this claim limitation in support of the obviousness rejection based on Conboy, Johnson, and Edwards.

Accordingly, given the record here, we reverse the rejections of independent claims 1, 8, 17, and 25, and their dependent claims 2–7, 9–16, 18–24, 26, and 27.

DECISION

For the reasons above, we reverse the Examiner's decision rejecting claims 1–27.

Claims Rejected	**Statute**	**References**	**Affirmed**	**Reversed**
1, 4–6, 8–10, 12–15	§ 103	Conboy, Johnson, Edwards		1, 4–6, 8–10, 12–15
2, 3	§ 103	Conboy, Johnson, Edwards, Clayton		2, 3
11	§ 103	Conboy, Johnson, Edwards, Pueblas		11
17–24	§ 103	Conboy, Johnson, Edwards, Svantesson		17–24
25	§ 103	Conboy, Johnson, Edwards, Currie		25
26	§ 103	Conboy, Johnson, Edwards, Stollman		26
27	§ 103	Conboy, Johnson, Edwards, Stollman, Epling		27
Overall Outcome				1–27

REVERSED