



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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for HE YUAN HUANG and examiner GEE, JASON KAI YIN.

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):

ibmptomail@iplawpro.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte HE YUAN HUANG, XIAO XI LIU, QI HU, and
GUAN QUN ZHANG

Appeal 2015-003274
Application 13/403,397
Technology Center 2400

Before JOHNNY A. KUMAR, JOHN A. EVANS, and
NATHAN A. ENGELS, *Administrative Patent Judges*.

ENGELS, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from a rejection of claims 1–20. No other claims are pending. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

ILLUSTRATIVE CLAIMS

Claims 1–3, reproduced below, are illustrative of the claimed subject matter:

1. A computer-implemented method for data leakage protection, comprising:

selecting, based upon communication between a user and a cloud application and from a plurality of monitoring templates, a monitoring template corresponding to the cloud application;

generating, using the selected monitoring template, a monitor;

obtaining, using the generated monitor, identifying information of content shared between the user and the cloud application; and

obtaining, according to the identifying information of the shared content, data about the shared content for security analysis.

2. The method of claim 1, wherein the monitor is configured to obtain information pertaining to a receiver of the content.

3. The method of claim 1, further comprising:

providing, according to the security analysis, interactive options, wherein the interactive options include at least one of

encrypting the sharing file,

adding a watermark, and

canceling an operation.

THE REJECTIONS

Claims 1–5, 10–14, 19, and 20 stand rejected under 35 U.S.C. § 102(b) as anticipated by Stringer et al. (US 2011/0212010 A1; Aug. 19, 2010).

Claims 6–9 and 15–18 stand rejected under 35 U.S.C. § 103(a) as unpatentable in view of Stringer and Letca et al. (US 2011/0167469 A1; July 7, 2011).

ANALYSIS

Having considered the Examiner’s rejections in light of Appellants’ arguments and the evidence of record, we disagree with Appellants that the Examiner erred. We agree with, and adopt as our own, the Examiner’s findings, conclusions, and reasoning and sustain the Examiner’s rejections. We provide the following analysis primarily for emphasis.

In the same field as Appellants’ “system for data leakage protection in cloud computing” (Spec. ¶ 2), Stringer’s disclosures relate to “detection of confidential data being transferred” (Stringer ¶ 2) in cloud computing (Stringer ¶ 6). More specifically, Stringer discloses systems and methods that “monitor application data input and outputs, where the system may detect sizeable exports of data from applications that are known to contain sensitive information.” Stringer ¶ 5. Among other things, Stringer discloses monitoring data output from a cloud-based application (Stringer ¶ 6) and triggering “a follow-up action . . . in response to the output data quantity being equal to or greater than [a] predetermined quantity” (Stringer ¶ 7). Examples of the follow-up actions include quarantining the output data,

providing content analysis to confirm the output data contains confidential information, and applying corporate data-management policies. Stringer ¶ 7.

The Examiner's Final Rejection cites to paragraphs 89 through 91 of Stringer as disclosing the "obtaining" steps of claim 1. *See* Final Act. 5; *but see* Final Act. 2–3 (providing analysis of paragraphs 89–91). Appellants argue the Examiner's block citation of those paragraphs fail to meet the notice requirements of 35 U.S.C. § 132 because the Examiner cites "paragraphs [0089]-[0091] and 'throughout' of Stringer without explanation." App. Br. 12; *see* App. Br. 5–6 (citing *In re Jung*, 637 F.3d 1356 (Fed. Cir. 2011)), 12–14; Reply Br. 2–3.

The Examiner responds to Appellants' lack-of-notice arguments by stating that the cited paragraphs, and the reference as a whole, show the disputed limitations clearly and need no further explanation. Ans. 2–3. Further, contrary to Appellants' arguments, the Examiner included additional analysis in the Response to Arguments section of the Final Rejection (*see* Final Act. 2–3) and in the Examiner's Answer (*see* Ans. 3–4).

We disagree with Appellants' arguments. As the Federal Circuit explained:

all that is required of the office to meet its prima facie burden of production is to set forth the statutory basis of the rejection and the reference or references relied upon in a sufficiently articulate and informative manner as to meet the notice requirement of § 132. As the statute itself instructs, the examiner must "notify the applicant," "stating the reasons for such rejection," "together with such information and references as may be useful in judging the propriety of continuing prosecution of his application."

Jung, 637 F.3d at 1363.

Further, § 132 “merely ensures that an applicant at least be informed of the broad statutory basis for the rejection of his claims, so that he may determine what the issues are on which he can or should produce evidence.” *Id.* (internal quotation omitted). Here, we find that the Final Office Action informed Appellants of the “broad statutory basis for the rejection of [Appellants’] claims” and provided sufficient information from which Appellants could identify issues and arguments to be addressed in this Appeal, as further discussed below.

Claim 1

Addressing the portions of Stringer cited in the Examiner’s rejection, Appellants argue Stringer applies data-monitoring filters and policies that are agnostic about the content of the data and Stringer does not, therefore, disclose the obtaining limitations of claim 1. App. Br. 14–15. Appellants argue Stringer’s filters and policies monitor for file size, file type, or an application type, not data content (App. Br. 14–15; *accord* Reply Br. 4), and, according to Appellants, “whether [a] document is a ‘.txt file, .doc file, [or] a database file’ fails to identify the shared content (i.e., the claimed ‘identifying information of the shared content’). Instead, the [file] type refers to a characteristic of a container (i.e., file) of the content.” Reply Br. 4.

We find that the plain language of claim 1 in light of Appellants’ Specification reads on Stringer’s disclosure. While Stringer does monitor and filter data output based on the quantity and type of data, we agree with the Examiner that the file size and type are examples of “data *about* the shared content.” *See* Final Act. 3; Ans. 3–4. Further, Stringer describes

additional examples of obtaining information about shared content, stating, for example, “certain data files may be associated with metadata indicating the sensitivity of information stored therein” and “[w]hen the application access[es] such a data file, that access indicates the application may have access to the sensitive data.” Stringer ¶ 89.

Moreover, we agree with the Examiner (*see* Ans. 3) that Stringer discloses obtaining identifying information of shared content as claimed with its disclosure of monitoring “characteristics of the data” and file types identifiable by filename extensions “(e.g. .txt file, .doc file, a database file, and so on),” which can trigger a follow-up action such as a quarantine, audit, and/or further analysis of the output data. *See* Stringer ¶¶ 7, 90–91. Indeed, rather than requiring the step of obtaining data content, claim 1 recites “obtaining . . . *identifying information* of [shared] content” and “obtaining . . . *data about* the shared content,” and we find nothing in the intrinsic evidence that warrants an interpretation to exclude the cited portions of Stringer (*cf.* Spec. ¶¶ 59 (describing “information relating to the content to be shared” as including “the sharing receivers and the identifier of the shared content”), 60 (describing a “monitor to capture the identifier of the content to be shared” and “according to the identifier thus obtained, the data of the content to be shared is obtained, and the data is sent to an analyzer for security analysis”). Accordingly, we sustain the Examiner’s rejection of claim 1.

Claim 2

Appellants argue Stringer does not teach “the monitor is configured to obtain information pertaining to a receiver of the content,” as recited in

dependent claim 2. App. Br. 16. The Examiner cites (*see* Ans. 4–5), and we agree, that Stringer’s disclosure of a monitor that applies file-access policies defined for “organization hierarchy, computer facility type, user type, network location . . . or the like” (Stringer ¶ 33) and a “destination address” (Stringer ¶ 97), for example, fall within the broadest reasonable scope of the claimed “information pertaining to a receiver of the content.” Appellants cite no intrinsic evidence that would require an interpretation of “information about a receiver” that would exclude Stringer’s disclosures, and Appellants’ arguments to the contrary amount to mere attorney argument. *See* Reply Br. 7 (“A destination address or destination point is not inherently (i.e., necessarily) information about a receiver (whether it be a human user or otherwise) of the content.”). Accordingly, we sustain the Examiner’s rejection of claim 2.

Claim 3

Appellants argue the Examiner erred in finding Stringer discloses the limitations of claim 3 because, according to Appellants, Stringer discloses preventing a connection and thus preventing content from being shared between a user and a cloud application. App. Br. 17–19; Reply Br. 8–10. We disagree with Appellants and agree with the Examiner that Stringer’s disclosure of, among other things, providing options to “stop further transmission of the data” fall within the scope of claim 3. *See* Ans. 6–7 (quoting Stringer ¶ 103; additionally citing Stringer ¶¶ 58, 91). Contrary to Appellants’ arguments (*see* Reply Br. 9–10), we agree with the Examiner that Stringer’s disclosure of stopping “further” transmission of “the data”

Appeal 2015-003274
Application 13/403,397

refer to data that is being shared. Accordingly, we sustain the Examiner's rejection of claim 3.

Claims 6–9 and 15–18

Appellants separately address the Examiner's obviousness rejections of claims 6–9 and 15–18, but Appellants do not advance independent arguments beyond those discussed above. Accordingly, we sustain the Examiner's rejection of claim 6–9 and 15–18 for the same reasons addressed above.

DECISION

We affirm the Examiner's rejections of claims 1–20.

No time period for taking any subsequent action in connection with this appeal may be extended. 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED