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.
14/408,178	12/15/2014	Kurt Essigmann	P45066-US1	8089

27045 7590 12/31/2018

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
DOLLY, KENDALL LYNN	

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
12/31/2018	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):

michelle.sanderson@ericsson.com
pam.ewing@ericsson.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte KURT ESSIGMANN, GERASIMOS DIMITRIADIS, and VOLKER KLEINFELD

Appeal 2018-005648
Application 14/408,178
Technology Center 2400

Before TERRENCE W. McMILLIN, KARA L. SZPONDOWSKI, and SCOTT B. HOWARD, *Administrative Patent Judges*.

McMILLIN, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) of the final rejection of claims 1–26. Final Act. 5. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

THE CLAIMED INVENTION

The present invention relates generally to "to the processing of messages for subscriber sessions," and more particularly "to the processing of a session-related message in a scenario in which a message originator and a destination of the message are located in different network domains." Spec. 1, ll. 9–12. Independent claims 1 and 18 are directed to methods and independent claims 21, 23, and 24 are directed to network elements. App. Br. 14, 18–21.

Claim 1, reproduced below, is representative of the claimed subject matter:

> 1. A method of processing a message for a subscriber session, the method comprising:
>
> Receiving, at a network element, a message, the message comprising a Fully Qualified Domain Name, FQDN, of an originator of the message, wherein the originator is located in a first network domain and wherein the message is directed towards a destination in a second network domain;
>
> determining, at the network element, the FQDN comprised in the message;
>
> determining, at the network element, an identifier associated with the message, wherein the identifier comprises at least one of a subscriber identifier, a session identifier and a destination identifier;
>
> applying, at the network element, a cryptographic operation on the FQDN and the identifier, or on information derived therefrom, to generate a cryptographic value;
>
> processing, at the network element, the message by substituting at least a portion of the FQDN with the cryptographic value; and
>
> forwarding, from the network element, the processed message towards the second network domain.

REJECTIONS ON APPEAL

Claims 1–26 stand rejected under 35 U.S.C. § 101 because the claimed invention is directed to patent-ineligible subject matter. Final Act. 4.

Claims 1–8 and 10–26 stand rejected under 35 U.S.C. § 103 as being unpatentable over Donovan (US 2013/0151845 A1; published June 13, 2013) and Mann et al. (US 2015/0046826 A1; published Feb. 12, 2015) ("Mann"). Final Act. 6, 19, 23.

ANALYSIS

35 U.S.C. § 101 Rejection

Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208 (2014), identifies a two-step framework for determining whether claimed subject matter is judicially excepted from patent eligibility under 35 U.S.C. § 101. In the first step, "[w]e must first determine whether the claims at issue are directed to a patent-ineligible concept." *Alice*, 573 U.S. at 218. In the second step, we "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (quoting *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66, 78–79 (2012)). In other words, the second step is to "search for an 'inventive concept' – *i.e.*, an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id.* (alteration in original) (quoting *Mayo*, 566 U.S. at 72–73).

The Examiner determines the claims are "directed to the abstract idea of *an idea of itself (i.e., the idea of collecting information, analyzing it, and displaying different results of the collection and analysis*: electric power group)." Final Act. 4; *see also* Ans. 4 (citing *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016)). According to the Examiner, the claimed "steps of receiving, determining and forwarding all relate to an abstract idea of data collection and/or data analysis," such as in *Electric Power Group*, where the "courts held that claims that do not go beyond the collection and analysis of information in a particular field, stating those function in general terms, without limiting them to a technical means for performing the functions define a desirable information based result and are not limited to inventive means of achieving the result." Ans. 4.

Appellants argue the claims are "directed to a method of processing a message for a subscriber session," and that the steps are "performed at a network element." App. Br. 8. Specifically, Appellants contend the "claims are directed to solving a problem that is rooted in inter network domain communication," and "provide a solution for how to process a message so that an external network domain is kept unaware of the internal architecture of the internal network domain" by "processing the message in a way that a cryptographic operation is applied [to] the FQDN and identifier of the message." *Id.* According to Appellants, the claimed receiving of a message, processing the message, and forwarding the processed message makes the network element "able to 'prevent topological information from leaving a dedicated network domain via outgoing messages.'" *Id.* Appellants argue, unlike in *Electric Power*, the "subject claims of this appeal do not simply

collect data for presentation to a user, rather it improves the processing of messages in a communications network." Reply Br. 2.

We agree with Appellants. We find the present claimed invention is more similar to the patent-eligible claimed invention in *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016) than to the patent ineligible claims in *Electric Power*. Specifically, our reviewing court has examined "whether the focus of the claims is on the specific asserted improvement in computer capabilities (i.e., the self-referential table for a computer database) or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." *Enfish,* 822 F.3d at 1335–36. In *Enfish*, the court highlighted that whether "the improvement is not defined by reference to 'physical' components does not doom the claims," and rather the "self-referential table recited in the claims on appeal is a specific type of data structure designed to improve the way a computer stores and retrieves data in memory." *Enfish*, 822 F.3d at 1339.

Here, as identified by Appellants, the claimed steps of processing a message in a way that the cryptographic operation is applied to the FQDN and identifier are performed at a network element. However, like in *Enfish*, the claimed steps performed at the network element are directed to improving computer function (i.e., solving a problem technologically rooted in inter network domain communication with a technologically rooted solution to process a message while hiding the internal architecture). *See* Spec. 10 ("the need for maintaining a mapping table that defines associations between pairs of internal and external host names can be avoided"). Like in *Enfish*, the claimed invention is not merely directed to generic computers performing generic computer functions that are otherwise

well-understood, routine, and conventional—which would not amount to significantly more than the abstract idea—but, instead, is directed to a specific improvement in computer capabilities (i.e., inter network domain communication). Such an improvement is not an abstract idea. *See Enfish*, 822 F.3d 1327.

Therefore, Appellants have persuasively established that the claimed invention is directed to a specific improvement in computer capabilities and should not be considered abstract.

Accordingly, we do not sustain the Examiner's 35 U.S.C. § 101 rejection of claims 1–26.

35 U.S.C. § 103 Rejection

Claim 1 recites "applying, at the network element, a cryptographic operation *on the FQDN and the identifier, or on information derived therefrom*, to generate a cryptographic value."

Appellants contend Donovan does not teach "applying a cryptographic operation on the *FQDN and the identifier*." App. Br. 10. Specifically, Appellants argue Donovan does not teach "also encrypting an identifier as recited in Claim 1," which "requires that the cryptographic operation be performed on the FQDN and the identifier." App. Br. 10; *see* App. Br. 11. According to Appellants, Donovan teaches "only a portion of the FQDN being encrypted," but "does [not] show how the identifier is included and the cryptographic operation is applied to both, together." App. Br. 10. Appellants further contend the claimed "'or on information derived therefrom' refers back to both the FQDN and the identifier – not just one of the FQDN or the identifier." Reply Br. 3. Specifically, Appellants argue the

"phrase 'or information derived therefrom' would include information derived from both the FQDN and identifier." Reply Br. 3–4. According to Appellants, "whenever the cryptographic operation is described [in] the *Application* it is always in the context of using at least portions of both the FQDN and an identifier," and therefore "both the FQDN and an identifier were to be used in the cryptographic operation." Reply Br. 3 (citing Spec. ¶¶ 16, 21, 78).

We are not persuaded by Appellants' arguments. Specifically, we agree with the Examiner's conclusion that, under broadest reasonable interpretation, the claim limitation includes that "the cryptographic operation can be performed on information derived therefrom" the FQDN and/or the identifier. Ans. 6. We further agree with the Examiner's finding that Donovan teaches applying a cryptographic operation on the domain and identifier, or information derived therefrom, to generate a cryptographic value. Final Act. 7 (citing Donovan ¶¶ 22, 23); *see* Ans. 7. According to the Examiner, Donovan teaches receiving a message with an origin host value as well as an origin realm value, and Donovan's received message teaches the claimed FQDN and identifier because "the message contains information pertaining to information relating to the originator," and that both the "origin host value as well as the origin realm value may both be encrypted." Ans. 7.

Appellants' Specification describes "[t]he cryptographic operation applied on the FQDN and the identifier, or an information derived from (such as a portion of the FQDN and/or a portion of the identifier), may comprise one or more operational steps." Spec. 4, ll. 19–21. Contrary to Appellants' argument (*see* Reply Br. 3), the Specification does *not* limit "or an information derived from" to using portions of *both* the FQDN and

identifier. The claimed "FQDN and the identifier, or . . . information derived therefrom" to which the cryptographic operation is applied, in light of the Specification, encompasses a portion of the FQDN *or* a portion of the identifier. Reply Br. 2.

As cited by the Examiner (*see* Final Act. 7), Donovan describes "[d]iameter agent 106 may be configured to encrypt the origin-host value in the request message" and "the origin-realm value in the ULR message may optionally be encrypted," with the example that "the Diameter ULR message is modified to include encrypted routing information indicated as 'Origin-Host=Encrypted(MME1).'" Donovan ¶ 22. Donovan also describes "[u]pon receiving the Diameter ULA message, Diameter agent 106 is configured to encrypt the origin-host AVP parameter value and subsequently replace the original origin-host AVP parameter value with the encrypted value." Donovan ¶ 23.

Appellants have not provided persuasive evidence or argument that the claimed applying a cryptographic operation to the FQDN and the identifier "or on information derived therefrom," encompassing a portion of the FQDN or a portion of the identifier, is not taught or suggested by Donovan's encrypting (i.e., applying a cryptographic operation to) the origin-host value and/or the origin-realm value (i.e., at least a portion of the FQDN).

Accordingly, we sustain the 35 U.S.C. § 103 rejection of independent claim 1, as well as independent claims 18, 21, 23, and 24, and dependent claims 2–8, 10–17, 19, 20, 22, 25, and 26, not separately argued. *See* App. Br. 12.

DECISION

The Examiner's rejection of claims 1–26 under 35 U.S.C. § 101 is reversed.

The Examiner's rejection of claims 1–8 and 10–26 under 35 U.S.C. § 103 is affirmed.

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

AFFIRMED-IN-PART