UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Case IPR2018-00067

Patent 8,577,813

UNIFIED PATENTS INC.,)

Petitioner,)

v.)

UNIVERSAL SECURE REGISTRY)

L.L.C.,)

Patent Owner.)

DEPOSITION OF ERIC BRIAN COLE

Reston, Virginia

Friday, December 14, 2018

REPORTED BY: Barbara DeVico, CRR, RMR

JOB NO. 152683

Friday, December 14, 2018
9:00 a.m.

Deposition of ERIC BRIAN COLE, held at the law offices of Regus, 11921 Freedom Drive, Reston, Virginia, pursuant to Notice before Barbara DeVico, Certified Realtime Reporter and Certified Nationally Certified Realtime Reporter and Registered Merit Reporter and Notary Public of the District of Columbia and the states of Maryland and Virginia.

APPEARANCES:
ON BEHALF OF PETITIONER:

MICHELLE CALLAGHAN, ESQUIRE
ERISE
5600 Greenwood Plaza Boulevard
Greenwood Village, CO 80111

ON BEHALF OF PATENT OWNER:
RAZMIG MESSERIAN, ESQUIRE
QUINN EMANUEL URQUHART & SULLIVAN
865 South Figueroa Street
Los Angeles, CA 90017

E. Cole

P R O C E E D I N G S

****

ERIC BRIAN COLE,

having been called as a witness on behalf of the Patent Owner and having been first duly sworn, was examined and testified as follows:

EXAMINATION BY
MR. MESSERIAN:

Q Good morning. My name is Razmig Messerian. I'm with the firm Quinn Emanuel, and I'm here on behalf of Universal Secure Registry LLC.

We are here to discuss the IPR for Patent No. 8,577,813; is that right?

A That's correct.

Q Could you please state your name for the record.

MR. MESSERIAN: You already got the name, right?

Q It seems like you've been deposed at least several times before?

A A few times, yes.

Q So I'm sure you're familiar with the ground rules, but let's go through them real quick anyhow.

E. Cole

You understand you're here to testify and you've taken an you oath, the same oath you've taken before?

A I do.

Q Is there anything that would interfere with your ability to testify today? For example, are you on any medication or anything like that that would affect your ability to testify?

A Okay. No. I am on medication but not that would impact my ability.

Q Do you understand that the court reporter is here to transcribe everything you say?

A Yes.

Q And to make that easier for her, it would be helpful if you could provide only audible responses and try not to make any hand gestures or nod your head yes or no to questions.

You understand that, right?

A I do.

Q And do you understand that it would be helpful to her if we don't talk over one another and let each other finish our sentences so she can transcribe what we say?

A Yes.

Q If at any point my questions are unclear

E. Cole

to you, will you let me know rather than just taking a wild guess?

A Yes, I will.

Q Great. So if I ask you a question and you answer it, I'm going to assume that you understood my question correctly. Is that fair?

A That is fair.

Q All right. If at any point you want to take a break, just let me know. I do ask that, if we're in the middle of a question, though, that we get an answer to it first and then we can take a break after that. Sounds good?

A Of course, I will let you know when I need a break well within 10 or 15 minutes so you can break when it's convenient.

Q Okay. Perfect. All right. So you can follow these rules for me, right?

A Yes, I can.

Q Okay. Did you speak with anyone to help you prepare for this deposition?

A Yes, I did.

Q Who did you speak to?

A With Michelle and with Jason from Erise IP.

E. Cole

Q Okay. Approximately how many hours would you say you spent speaking to them about preparing for this deposition?

I'm sure you didn't take, you know, detailed records of it. But just roughly speaking, was it a day? Was it more than a day? Less than a day?

A It was multiple one- to two-hour sessions over a few days.

Q Okay.

A So I'm guessing a total of maybe eight to ten hours.

Q Got it. And did you review any documents to prepare for this deposition?

A Yes, I did.

MS. CALLAGHAN: I would just counsel that -- not to reveal any privileged communications between you and counsel.

THE WITNESS: Okay.

MS. CALLAGHAN: Thanks.

BY MR. MESSERIAN:

Q Sorry. You said you reviewed some document, right, to prepare for this deposition?

A Yes.

Q What -- what sort of documents did you

E. Cole

review?

A I reviewed my two reports that I wrote and the patents.

Q Okay. Prior art patents as well, Maes, Labrou, Gullman, Weiss?

A Correct.

Q So you mentioned you prepared a couple of reports.

One of those reports was in support of Petitioner's Reply to Patent Owner Response, and the other one was in support of Petitioner's Opposition to Motion to Amend; is that right?

A That sounds correct, yes.

Q Did you prepare these declaration -- or these reports, or defendant's counsel prepare them for you and you reviewed them for accuracy?

MS. CALLAGHAN: Same objection as before -- or same counsel as before.

A I worked with counsel on preparing them, so I wrote sections. We did talk and discuss various aspects of it, but all of the opinions in the report are my opinions.

Q Okay. So you're familiar with everything in there? You understand them, right?

E. Cole

A Yes. I don't have them memorized, but I am familiar with everything in my report.

Q Of course. Okay.

All right. So let's turn to some of these prior art references. In particular, I want to turn to Labrou first.

A Okay.

MR. MESSERIAN: All right. So I'd like to mark U.S. Patent Publication 2004/0107170, which is the Labrou reference, as Exhibit 1 in this deposition. The Labrou reference is Exhibit 1005 in the IPR.

(Exhibit 1, U.S. Patent Publication 2004/0107170, was marked for identification.)

BY MR. MESSERIAN:

Q Is that the Labrou reference there? Does that look like the one you reviewed?

A Yes, it does.

Q All right. When's the last time you reviewed this reference?

A I'd have to go back and check. I mean, I briefly looked at it.

Q Have you looked at it in the last week?

A I went through my report in the last week

E. Cole

and looked at everything in the report.

Q Okay.

A I might have glanced. But in going through it in detail, it might have sometime over the last month when I worked on the report.

Q Okay. Nevertheless, would you say you've spent sufficient time reviewing Labrou so that you have a good understanding generally what it teaches?

MS. CALLAGHAN: Objection. Form.

A Yes. So in putting together my reports, I reviewed the Labrou patent.

Q All right. Could you please turn to paragraph 527.

A (Witness complies with request.)

Q It's on page 30.

Could you please read the first several sentences -- the first four or five sentences.

A Which paragraph?

Q 527.

A 527.

(Witness complies with request.)

Q Is it fair to say that Labrou there describes how a random sequence number, RSN, is generated using a pseudorandom sequence number

E. Cole

function R?

MS. CALLAGHAN: Objection. Form.

A I believe you're referring to the first sentence, "The RSN is a pseudorandom number that is generated from a locally stored pseudorandom sequence number function R."

Q Great. All right. Does Labrou also describe any input to that function R?

A If you go down about four or five lines, it says, "Typically, the generation of a pseudorandom number also involves another parameter, a seed S. The seed S is used as the initial input parameter for the generator R to generate its first pseudorandom number output."

Q Great. So it uses initial seed value S, input into a function R, and it generates the RSN; right?

MS. CALLAGHAN: Objection. Form.

A That is my understanding from reading paragraph 527.

Q Great. All right. Could you please read the rest of 527 if you haven't read the entire thing.

A (Witness complies with request.)

Q Based on what you just read, would you

E. Cole

agree that the function R and the original seed value S are stored at the agreement AP party -- agreement party, AP party?

MS. CALLAGHAN: Objection. Form.

A I believe you're referencing each AP device as its own R and S, which are securely stored on the device and at the AVP.

Q All right. So Labrou, at least in this paragraph, talks about storing that original seed value S at the agreement party device.

But does it also say anything about where that seed S is obtained or derived?

MS. CALLAGHAN: Objection. Form.

A Specifically in paragraph 527, it does not look like it provides details on where S is generated.

Q Okay. Fair enough. This paragraph also talks a little bit about the device identifier, DID.

What does Labrou there say a verification server, AVP, agreement verification party, does with that device identifier, DID, value?

MS. CALLAGHAN: Objection. Form.

A "On the AVP, given the DID of an AP device by which an RSN is generated, a program can

E. Cole

deterministically locate the same pseudorandom function generated function R and the corresponding pseudorandom number generation seed S for that device from the user and device database containing information about all issued devices."

Q Okay. So based on that and based on rest of paragraph 527 that you just read, regarding the device identifier, DID, does Labrou there say anything about that device identifier, DID, being used to derive or obtain the original seed value S?

MS. CALLAGHAN: Objection. Form.

A Specifically, in paragraph 527, it just talks about locating the corresponding pseudorandom generation seed S. It does not provide specific details of how this is generated.

Q Okay. Fair enough. To your knowledge and understanding -- this is a huge reference -- do you remember or do you recall any other portion of Labrou discussing how that original seed value S is derived or specifically it being derived from a DID?

MS. CALLAGHAN: Objection. Form.

A I would have to go back and look at my reports. I don't have those memorized, so I would have to go back and look to verify that.

E. Cole

Q Okay. Fair enough. Let's move on.

Actually, before we move on, let's talk a little bit more about that seed that we were just talking about, that original seed value S.

Does it say anything about it being fixed, or does it vary in time? Does it say anything about that?

A Specifically, in paragraph 527, I do not see any reference to the seed, I mean, being fixed. But that's only specific to paragraph 527. I would need to look through my reports to completely answer that, but I can reference it specifically in 527.

Q All right. Could you please go and flip a couple pages and read paragraphs 537 and 538.

A (Witness complies with request.)

Q Can you, in your own words, explain to me what's discussed in those two paragraphs.

A And just to confirm, paragraph 537 and 538?

Q That's right.

A A hash function is a type of cryptographic function that performs what you call a one-way transformation. So it's saying that it's difficult to invert -- is once you create the hash, it's difficult, with the hash, to get back the original

E. Cole

value.

So what they're doing here is they're taking the hash function and applying it to the two-argument function F, apply it to the locally generated RSN in the PIE input by the user to create a single output or a single argument.

Q Very well said. That two-argument function, does Labrou give any examples of what that function could be?

MS. CALLAGHAN: Objection. Form.

A Specifically, in paragraphs 537 and 538, I do not see Labrou give any specific examples of functionality.

Q Okay. At the bottom of 538, could you read that last sentence starting with "The function."

A "The function can be any known function, such as a function that appends the PIE string to the RSN string or XORs the PIE and the RSN."

Q Okay. So would you then agree that that two-argument function F, here Labrou talks about how you could use an XOR operation as that function?

A Yes.

Q Okay. You mentioned earlier that a cryptographic one-way hash function makes it very

E. Cole

difficult to invert the output to get back the input, right? Or if you want to say it in your own words again...

A I would agree with that --

Q Okay.

A -- definition.

Q What is the output of that hash function in this case?

A The output is a single argument, typically a string, in order to create the encryption key K.

Q Okay. And below that, we have an equation, K=H(F)(PIE, RSN).

So K there is the encryption key K, right, in that formula?

A Yes.

Q So the output of that hash function is the encryption key K. Is that fair to say?

A Yes.

Q If I gave you that encryption key K after it's been hashed and generated and then I gave it to you, could you somehow take that key, apply the PIE value to it somehow, and reversibly determine what the other argument was, the RSN value?

E. Cole

MS. CALLAGHAN: Objection. Form.

A I just want to make sure. Are you saying that, if I take the output of the hash and give it one of the several inputs, would I be able to figure out the other inputs?

Q That's correct. That's my question.

A Okay. With a hash function, typically no. That's the point of doing a one-way transformation.

Q All right. At this point, let's move on past the Labrou reference. I think we're going to come back to this a little bit later, so we can keep it somewhere handy.

MR. MESSERIAN: All right. Next I'd like to mark U.S. Patent 6,016,476, which is the Maes reference, as Exhibit 2 in this deposition. The Maes reference is Exhibit 1003 in the IPR.

(Exhibit 2, U.S. Patent 6,016,476, was marked for identification.)

BY MR. MESSERIAN:

Q Is this the Maes here that I'm handing you now that you're familiar with?

A Yes.

Q Same question as before: When was the

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.