

[seal]

Certified Copy

FEDERAL PATENT COURT

IN THE NAME OF THE PEOPLE

JUDGMENT

2 Ni 26/16 (EP)
combined with
2 Ni 46/16 (EP)

Announced on
July 12, 2018

Zindler
Judicial Employee
acting as
Clerk of the Court

(File Reference)

In the patent nullification matter

1. Hewlett-Packard GmbH, Herrenberger Strasse 140, D-71034 Böblingen,
legally represented by its Executive Directors Thomas Bässler,
Marc Fischer, Heiko Meyer and Ernst Reichart, *ibid*,

Plaintiff on 1,

2. Huawei Technologies Deutschland GmbH, Hansaallee 205, D-40549
Düsseldorf, legally represented by its Chief Executive Officer Bo Peng,
ibid,

Plaintiff on 2,

Plaintiffs in the Proceeding 2 Ni 26/16 (EP),

Attorney for this proceeding of Plaintiffs on 1 and 2: Klunker IP, Patent Attorneys
PartG mbB, Destouchesstrasse 68, D-80796 Munich

BPatG 253
05/08

3. Sandvine GmbH, Fürstenrieder Strasse 263, 81377 D-Munich,
legally represented by its Chief Executive Officer Richard Arthur Murphy Deggs, *ibid*,
Plaintiff on 3,
Plaintiffs in the Proceeding 2 Ni 46/16 (EP),

Attorney for this proceeding: Preu Bohlig & Partner Rechtsanwälte mbB
Grolmanstrasse 36, D-10623 Berlin,

vs.

Packet Intelligence LLC, 505 East Travis Street, Suite 209, Marshall, Texas 75670
United States of America

Defendant,

Attorney for this proceeding: MFG Patentanwälte Meyer-Wildhagen Meggle-Fruend Gerhard
PartG mbB, Amalienstrasse 62, D-80799 Munich

regarding European Patent 1 196 856

(DE 600 45 552)

the Second Senate (Nullification Senate) of the Federal Patent Court, on the basis of the oral hearing of July 12, 2018, with the cooperation of Chief Judge Guth as well as Judge Dipl.-Ing Baumgardt, Judge Dipl.-Phys Dr. Thum-Rung, and Judges Dipl.-Phys. Dr. Forkel and Dr. Himmelmann,

has ruled:

- I. European Patent 1 196 856 is declared null and void with effect on the sovereign territory of the Federal Republic of Germany.

- II. The Defendant shall bear the costs of the legal proceeding.
- III. The judgment is provisionally enforceable against payment of security in the amount of 120% of the enforced amount.

Facts of the Matter

The Defendant is the holder of the Patent **EP 1 196 856 B1** applied for on June 30, 2000 and published on January 19, 2011 (hereinafter: the Patent in Suit) which is designated “METHOD AND APPARATUS FOR MONITORING TRAFFIC IN A NETWORK” (German: “Verfahren und Gerät um den Netzwerkverkehr zu überwachen”), which originates with the international application with Publication Number WO 2001/1 272 A1, and is asserted for the priority of U.S. Application 60/141 903 of June 30, 1999. The Patent in Suit written in the English language is maintained by the German Federal Patent and Trademark Office under Number DE 600 45 552.1.

The Plaintiffs each request by their pleadings the nullification in full of the German portion of the European Patent.

The Defendant defends its Patent in Suit in full by its Primary Application, and alternatively limits this with Alternative Applications 1, 2a-d and 4, each dated January 8, 2018, as well as with Alternative Applications 2e, 3 and 5-9 dated May 28, 2018.

The Patent in Suit is comprised of 92 patent claims, with a Primary Application directed to a “Method for recognizing one or more communications, for packets passing through a node point in a computer network”, and 39 sub-claims referring to it, as well as with a coordinate Claim 41 directed to a “packet

monitor” set up for this purpose, and 51 sub-claims referring to it.

In the English language proceeding, the granted independent Patent Claims 1 and 41 are worded according to the specification of the Patent in Suit EP 1 196 856 B1:

“1. A method of recognizing one or more conversational flows for packets passing through a connection point (121) on a computer network (102), each packet conforming to at least one protocol, wherein at least one said protocol defines one or more conversational flows that each includes a plurality of states of the flow including an initial state, and transitions from the initial state to at least one of the plurality of states of the flow, the method comprising:

receiving a packet (302) from a packet acquisition device;

performing at least one parsing operation (304) and/or at least one extraction operation (306) on the packet to create a parser record comprising a function (312) of selected portions of the packet; wherein at least one of the parsing and/or extraction operations depend on one or more of the protocols to which the packet conforms; looking up (314) in a flow-entry database (324) comprising flow entries for any previously encountered conversational flows, the look up using at least some of the selected packet portions and determining (316) if the packet is of an existing conversational flow;

if the packet is of an existing conversational flow, classifying the packet as belonging to the found existing conversational flow and performing (328, 330) any state operation or operations specified in a database (326) for the state of the conversational flow; and

if the packet is of a new conversational flow, storing (322) a new flow-entry for the new conversational flow in the flow-entry database, including identifying information for future packets to be identified with the new flow-entry, determining the state of the flow (318) using the database (326) and

performing (328, 330) any state operation or operations specified in the database (326) for the state of the flow;

wherein each conversational flow that includes a plurality of states is recognized by transitioning through a plurality of states of the conversational flow, and at each state, carrying out one or more state operations specified in the database (326) for the state of the flow.”

“41. A packet monitor (108) for recognizing one or more conversational flows for packets passing through a connection point (121) on a computer network (102), each packet conforming to at least one protocol, wherein at least one said protocol defines one or more conversational flows that each includes a plurality of states of the flow including an initial state, and transitions from the initial state to at least one of the plurality of states of the flow, the packet monitor comprising:

a packet acquisition device (1502) for coupling to the connection point and configured to receive packets passing through the connection point, including an input buffer memory (1008) coupled to and configured to accept a packet;

a parser subsystem (301) coupled to the input buffer memory and including a slicer (1007), the parsing subsystem configured to extract selected portions of the received packet and to output a parser record containing the selected portions, wherein the operation of the parser subsystem depends on one or more of the protocols to which the packet conforms;

a memory (324) for storing a database comprising flow-entries for any previously encountered conversational flows, each flow-entry identified by identifying information stored in the flow-entry, conversational flows having one or more states;

a lookup engine (1107) coupled to the output of the parser subsystem and to the memory and configured to lookup whether the particular packet whose parser record is output by the parser subsystem has a matching flow-entry in

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.