NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

AMAZON.COM, INC., AMAZON.COM, LLC, AMAZON WEB SERVICES, INC., BAZAARVOICE, INC., GEARBOX SOFTWARE, LLC,
Appellants

v.

ZITOVAULT, LLC,
Appellee

2017-2147

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2016-00021, IPR2016-01025.

Decided: November 16, 2018

DAN L. BAGATELL, Perkins Coie LLP, Hanover, NH, argued for appellants. Also represented by GRANT EDWARD KINSEL, Los Angeles, CA; CHRISTINA JORDAN MCCULLOUGH, JONATHAN R. PUTMAN, Seattle, WA.

JUSTIN NEMUNAITIS, Caldwell Cassady & Curry, Dallas, TX, argued for appellee. Also represented by

JASON DODD CASSADY; MICHAEL RAYMOND CASEY, Oblon, McClelland, Maier and Neustadt, LLP, Alexandria, VA.

Before PROST, *Chief Judge,* O'MALLEY and STOLL, *Circuit Judges.*

Opinion for the court filed by *Circuit Judge* STOLL.

Dissenting Opinion filed by *Chief Judge* PROST.

STOLL, *Circuit Judge.*

Amazon.com, Inc., Amazon.com, LLC, Amazon Web Services, Inc., Bazaarvoice, Inc., and Gearbox Software, LLC, (collectively, "Amazon"), appeal from a final written decision of the Patent Trial and Appeal Board in which the Board held that Amazon failed to prove ZitoVault, LLC's U.S. Patent No. 6,484,257 unpatentable. The Board did not err in its claim construction, and it correctly held Amazon to its burden of proof. Because it did not err in finding Amazon failed to carry that burden and because it did not violate Amazon's procedural due process rights, we affirm.

BACKGROUND

ZitoVault's '257 patent seeks to improve computer systems' handling of encrypted communications. *See* '257 patent col. 3 l. 65–col. 4 l. 1. Rather than using a single "main" server to decrypt every communication, the disclosed system also enlists the computers receiving the communications as decryption agents, thereby avoiding bottlenecks, as shown in Figure 2.

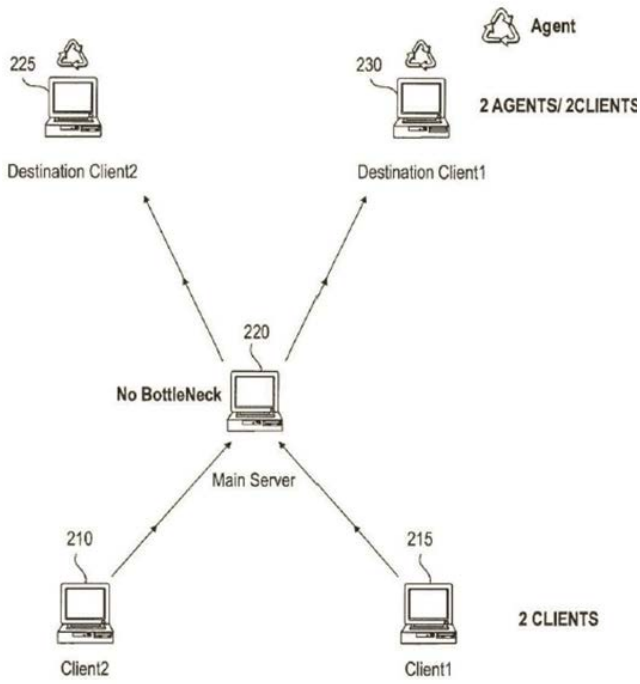

Fig. 2

Id. at Fig. 2; *see also id.* at col. 7 ll. 21–34. Representative claims 1 and 6 describe the claimed invention:

> 1. A system for conducting a plurality of cryptographic *sessions* over a distributed network of computers, employing a distributed automaton running on the network comprising M agents for servicing N number of simultaneous cryptographic *sessions* wherein bandwidth and number of *sessions* are scalable by the M agents and latency is potentially reducible to zero comprising:
>
> a main server;
>
> one or more clients communicating over the distributed network with said main server and agents;

> M agents communicating with the main server for enlisting additional agents to support incremental cryptographic *sessions* with the clients to maintain system performance at a desired level; and for encrypting and decrypting communication traffic as it arrives from the clients via the main server, the agents comprising a single-to-many connection (1 client, M agents) with respect to the clients, such that portions of the bandwidth are equally divided among the M agents for processing, and the agents combine the processing power of all computers connected to the system to service encryption and decryption and enable bandwidth to be scalable by the M agents and to reduce latency substantially to zero.
>
> ***
>
> 6. A method for implementing a scaleable software crypto system between a main server and one or more agent servers communicating with one or more clients such that performance of the crypto system is increased to meet any demand comprising
>
> providing a secure communication between the main server, agent server, and one or more clients such that communication between the main server and agent server enlists additional agent servers to support incremental secure *sessions* in response to maintaining performance at a desired level.

Id. at claims 1, 6 (emphases added to highlight disputed claim term).

After ZitoVault sued Amazon for infringement, Amazon petitioned for inter partes review of the '257 patent. Amazon raised three grounds of unpatentability, each

based on U.S. Patent No. 6,065,046 ("Feinberg"), and each instituted by the Board.

Over the course of the IPR, the parties' dispute crystalized around the issue of whether Feinberg discloses the claimed "sessions." Amazon relied on Feinberg for every claim limitation reciting "sessions." But Amazon did not delineate exactly where Feinberg describes the claimed sessions and did not explain what constitutes a session in Feinberg's system. Amazon also did not propose a construction of "sessions," but its expert testified that a "session generally refers to one or more communications exchanged between two entities over some period of time." J.A. 540.

At the institution stage, the Board accepted Amazon's contention that Feinberg discloses "sessions." Citing a telecommunications dictionary, it preliminarily construed "sessions" as "a set of transmitters and receivers, and the data streams that flow between them." J.A. 180. It found that "based on that construction, the mere exchange of data (e.g., encrypted code modules), as disclosed in Feinberg, falls within the scope of the claimed *sessions*." *Id.*; *see also* J.A. 185–86 ("[W]e adopt a broader construction of the term 'session' that encompasses simply the exchange of [data] packets.").

In its Patent Owner Response, ZitoVault maintained that Feinberg lacked the claimed sessions. It offered expert testimony that a "session" "must refer to a connection with a defined beginning and end" so that the server can determine which incoming data belongs to which session. J.A. 219–20, 1184–86. ZitoVault further contended that Amazon's petition was defective because it "fail[ed] to specifically identify what it contends is the 'session' in Feinberg or how that session is initiated, maintained, or terminated." J.A. 235. ZitoVault separately urged the Board to find that a reference must disclose "negotiating the initiation of a stream with a

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.