Trials@uspto.gov
571-272-7822

Paper 9
Date Entered: May 2, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE INC.,
Petitioner,

v.

ALFONSO CIOFFI, MEGAN ELIZABETH ROZMAN,
MELANIE ANN ROZMAN, AND MORGAN LEE ROZMAN,
Patent Owners.

Case CBM2017-00015
Patent RE43,528

Before JAMESON LEE, BRIAN J. McNAMARA, and
CHRISTOPHER M. KAISER, *Administrative Patent Judges.*

McNAMARA, *Administrative Patent Judge*.

DECISION
Institution of Covered Business Method Patent Review
37 C.F.R. § 42.208

BACKGROUND

Pursuant to 35 U.S. C. § 321 and section 18 of the America Invents Act (AIA), Google, Inc. (Petitioner) filed a Petition, Paper 1 ("Pet."), requesting that the Patent Trial and Appeal Board initiate a covered business method patent review of claims 1, 5, 8, 21–24, 30, 44, 64, and 67 (the "challenged claims") of U.S. Patent RE43,528 (the '528 Patent). Petitioner contends that pursuant to 37 CFR §§ 42.301 and 42.304(a) the '528 Patent meets the definition of a covered business method patent and does not qualify as a technological invention. Pet. 5–16. Petitioner also contends that the challenged claims are unpatentable over the prior art. *Id.* at 29–61.

Alfonso Cioffi, Megan Elizabeth Rozman, Melanie Ann Rozman, and Morgan Lee Rozman (collectively, "Patent Owner") filed a Patent Owner Preliminary Response contesting Petitioner's assertion that the '528 Patent is a CBM patent and the grounds on which Petitioner challenges the patentability of the claims. Paper 5 ("Prelim. Resp.").

The standard for instituting a covered business method patent review is the same as that for a post-grant review. (§ 18(a)(1) of the AIA). For the reasons discussed below, we are not persuaded that Petitioner has demonstrated that the '528 Patent is a CBM patent. Therefore, we do not institute a covered business method patent review.

PENDING LITIGATION

A person may not file a petition under the Transitional Program for Covered Business Method Patents unless the person or the person's real party in interest or privy has been sued for infringement or has been charged

with infringement under that patent. *See* § 18(a)(1)(B) of the Leahy-Smith America Invents Act, Pub. L. 112-29, 125 Stat. 284, 329 (2011) ("AIA"). Petitioner represents that it has been sued for infringing the '528 Patent in *Cioffi, et al. v. Google Inc.*, 2:13-cv-00103 (E.D. Tex.). Pet. ix.

THE '528 PATENT (EXHIBIT 1001)

The '528 Patent is a reissue patent of U.S. Patent No. 7,484,247. Ex. 1001, 1:14–15. As its title indicates, the '528 Patent discloses a system and method for protecting a computer from malicious software. Figure 1 illustrates a computer system with first and second processors 120 and 140, respectively. As Figure 1 of the '528 Patent shows, both processors 120 and 140 have a direct communication link with second memory 130, but only first processor 120 has a direct communication link with first memory 110. Second processor 140 can access memory 110, as in a multicore system, using processor 120 only with strict user permission through real time interaction or via stored configurations or commands. *Id.* at 10:37–44. Figure 1 shows network interface 190, such as a router or gateway, communicating with second processor 140 and the network. *Id.* at 10:13–18. Decryption keys can be passed between first processor 120 and network interface device 190 via communication link 191. *Id.* at 17:31–33. Figure 1 also shows that user interface 150 provides input to first processor 120 and communicates with video processor 170 via link 151. Video processor 170 communicates with first processor 120 via link 171 and with second processor 140 to provide information to video display 180 and is adapted to combine video data from the first and second processors and transmit it to display terminal 180 for display in a windowed format. *Id.* at 8:31–35.

This architecture is designed to protect memory 110 from malware initiated intrusions and from initiating unwanted processes on first processor 120 by using second processor 140 to isolate first processor 120 and memory 110 from network 195. Ex. 1001, 8:35–39, 10:20–37. The flow diagram in Figure 3 illustrates a basic process in which a user selects data files to download via a browser (step 310) and second processor P2 downloads and writes the data files to second memory M2 (step 320). When first processor P1 is directed to move the data files from memory M2 to first memory M1 (step 330), processor P2 scans for malware in the downloaded data file (step 340). Depending on whether or not malware is detected (step 350), the data file is copied to memory M1 (step 360) or quarantined on memory M2 (step 370) and deleted, cleaned or otherwise quarantined on M2 (step 380). Variations of this process are shown in Figures 4–6 and 10. Figures 7–9 illustrate various processor configurations. For example, Patent Owner notes that Figure 9 shows processor 960 with multiple cores, i.e. first processor core 920 and second processor core 940 and separate isolated memory areas 910 and 930 within a single memory space. Prelim. Resp. 6–7. Processor core 920 can access memory areas 910 and 930 and second processor 940 can access memory area 930 and may be configured to be incapable of initiating access to memory area 910. *Id.* Functions carried out by processors 920 and 940 may be separate logical processes operating on the same processor, but functions carried out by second processor 940 may be configured as unable to access automatically first memory area 910 or second memory area 910 or another logical process performing functions of first processor 920. *Id*. at 7–8 (citing Ex. 1001 16:10–12, 22–31).

ILLUSTRATIVE CLAIM

Claim 1 is illustrative and is reproduced below as it appears in the '528 Patent, with matter enclosed in heavy brackets **[ ]** appearing in original U.S. Patent No. 7,484,247, but forming no part of the reissue '528 Patent and matter in italics indicting additions made by reissue.

1. A method of operating a computer system *capable of exchanging data across a network of one or more computers and* having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising **[**the steps of**]**:

executing **[**instructions**]** *a first web browser process, capable of accessing data of a website via the network,* in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space **[**and a second memory space**]**;

executing **[**instructions**]** *a second web browser process* in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space **[**, the second logical process being further capable of exchanging data across a network of one or more computers**]**;*and*

displaying**[**, in a windowed format on a display terminal,**]** data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to **[**the**]** *a* display **[**terminal**]**;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second **[**logical**]** *web browser* process.

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.