NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

KINGSTON TECHNOLOGY COMPANY, INC.,
Appellant

v.

SPEX TECHNOLOGIES, INC.,
Appellee

2019-1256

Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board in No. IPR2017-01021.

Decided: February 21, 2020

DAVID M. HOFFMAN, Fish & Richardson, P.C., Austin, TX, argued for appellant. Also represented by OLIVER RICHARDS, San Diego, CA.

KRISTOPHER DAVIS, Russ August & Kabat, Los Angeles, CA, argued for appellee. Also represented by MARC AARON FENSTER, PAUL ANTHONY KROEGER, BENJAMIN T. WANG.

Before DYK, O'MALLEY, and STOLL, *Circuit Judges*.

STOLL, *Circuit Judge*.

Kingston Technology Company, Inc. appeals the Patent Trial and Appeal Board's final written decision declining to find claims 55–57 of U.S. Patent No. 6,003,135 anticipated by PCT Application WO 95/16238 (Jones). Because substantial evidence supports the Board's determination that Jones does not expressly or inherently disclose certain limitations of claims 55 and 56, we affirm as to those claims. With regard to claim 57, we hold that the Board abused its discretion when it rejected Kingston's supplemental briefing for purportedly presenting a new theory of invalidity. We therefore vacate the Board's decision as to claim 57 and remand for the Board to consider Kingston's supplemental briefing addressing claim 57.

BACKGROUND

I

The '135 patent, titled "Modular Security Device," is directed to a modular, typically portable, device that communicates with a host computing device—e.g., a host computer. The disclosed modular device contains a security module and a target module. The security module provides security functionality such as encryption or password control, while the target module provides non-security functionality such as data storage, biometric scanning, a modem, or a smart card reader. The '135 patent discloses that separating the security elements of the modular device from other functionality provides for a single security module that can be used to provide security to multiple types of interactions with the host computer.

In certain embodiments, the security module can be positioned inline such that all communications between the target module and the host computer must travel through it. The same security module can also be used with a variety of target modules, thereby increasing flexibility. In addition, the modular device can be implemented to assume

the identity of the target module such that the security module is transparent to the host computer.

Claims 55 and 57 are illustrative:

> 55. For use in a modular device adapted for communication with a host computing device, the modular device comprising a security module that is adapted to enable one or more security operations to be performed on data and a target module that is adapted to enable a defined interaction with the host computing device, a method comprising the steps of:
>
> *receiving a request from the host computing device for information regarding the type of the modular device*;
>
> *providing the type of the target module to the host computing device in response to the request*; and
>
> operably connecting the security module and/or the target module to the host computing device in response to an instruction from the host computing device.
>
> . . .
>
> 57. For use in a modular device adapted for communication with a host computing device, the modular device comprising a security module that is adapted to enable one or more security operations to be performed on data and a target module that is adapted to enable a defined interaction with the host computing device, a method comprising the steps of:
>
> *communicating with the host computing device to exchange data between the host computing device and the modular device*;

> *performing one or more security operations and the defined interaction on the exchanged data*;
>
> mediating communication of the exchanged data between the host computing device and the modular device so that the exchanged data must first pass through the security module; and
>
> operably connecting the security module and/or the target module to the host computing device in response to an instruction from the host computing device.

'135 patent col. 26 ll. 12–53 (emphases added to highlight disputed claim limitations).

The specification of the '135 patent explains that some embodiments conform to the PCMCIA standard. PCMCIA cards, popularized in the 1990s, were removable modules with a variety of functions—e.g., modem, smart card reader, data storage—that could be inserted into a designated slot in a laptop computer. The Personal Computer Memory Card International Association established the standard for PCMCIA cards (hence the name),[1] and the PCMCIA standard is comprised of multiple discrete specifications.

II

Jones is the only prior art reference at issue on appeal. Jones is a PCT Application directed to "[a] detachable PCMCIA memory card . . . incorporating a smartcard integrated circuit." Jones at Abstract. The memory card of Jones provides removable data storage secured by a password, encryption, or both.

Jones discloses at least one embodiment that conforms to the PCMCIA standard. Jones specifically cites to the

---

[1] PCMCIA cards were later dubbed "PC Cards."

"PC Card Standard Specification, Release 2.01, published in November, 1992," but does not expressly incorporate that specification by reference. Jones col. 5 ll. 22–23; *see also id.* at col. 8 ll. 26–29 (similar). Elsewhere, Jones explains that "[t]he programming interface to the PCMCIA Card Services software is defined in Section 3 of the PCMCIA Standard (Release 2.01)," but again does not expressly incorporate that disclosure by reference. *Id.* at col. 9 ll. 16–19.

III

Kingston petitioned for inter partes review of claims 55–58 of the '135 patent based on anticipation by Jones, obviousness over Jones alone, and obviousness over Jones in view of other prior art. The Board initially declined to institute review for claims 55–57, but modified its institution decision to include those claims following *SAS Institute, Inc. v. Iancu*, 138 S. Ct. 1348 (2018). The Board then permitted Kingston to submit supplemental information pursuant to 37 C.F.R. § 42.123. The Board also authorized the parties to file supplemental briefing addressing the supplemental information submitted by Kingston.

The Board issued a final written decision in which it held claim 58 unpatentable, but declined to hold claims 55–57 unpatentable. *See generally Kingston Tech. Co. v. SPEX Techs., Inc.*, No. IPR2017-01021, 2018 WL 4773543, at *1 (P.T.A.B. Oct. 1, 2018) ("*Decision*"). Relevant here, the Board found that Kingston had failed to show by a preponderance of the evidence that claims 55–57 of the '135 patent are anticipated by Jones.[2] In so finding, the Board declined to consider Kingston's supplemental

[2] Although not at issue on appeal, the Board also rejected Kingston's obviousness arguments based on Jones alone and in combination with other references.

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.