NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

NEOLOGY, INC.,
Appellant

v.

INTERNATIONAL TRADE COMMISSION,
Appellee

KAPSCH TRAFFICCOM USA, INC., KAPSCH TRAFFICCOM HOLDING CORP., KAPSCH TRAFFICCOM CANADA INC., STAR SYSTEMS INTERNATIONAL LTD., STAR RFID CO., LTD.,
Intervenors

2018-1338

Appeal from the United States International Trade Commission in Investigation No. 337-TA-979.

Decided: April 19, 2019

VINAY VIJAY JOSHI, Amin Turocy & Watson LLP, San Jose, CA, argued for appellant. Also represented by DANIEL W. BEDELL, ANTHONY KIM, ANDREW TIMOTHY OLIVER.

CATHY CHEN, Office of the General Counsel, United States International Trade Commission, Washington, DC, argued for appellee. Also represented by DOMINIC L. BIANCHI, WAYNE W. HERRINGTON, SIDNEY A. ROSENZWEIG.

NATHAN S. MAMMEN, Kirkland & Ellis LLP, Washington, DC, argued for intervenors. Also represented by GREGG F. LOCASCIO, BRIAN H. GOLD.

Before TARANTO, SCHALL, and CHEN, *Circuit Judges.*

TARANTO, *Circuit Judge.*

Neology filed a complaint with the International Trade Commission in 2015, alleging, as now relevant, infringement of claims 13, 14, and 25 of its U.S. Patent No. 8,325,044 and claims 1, 2, and 4 of its U.S. Patent No. 8,587,436. The patents, which share a specification, describe and claim systems and methods for tracking identifying information, particularly those relying on radio frequency identification (RFID). The Commission held the claims now at issue invalid because (1) they lack adequate written description support and (2) they are invalid for anticipation by U.S. Patent No. 5,627,544 (Snodgrass) or for obviousness based on the combination of Snodgrass and two other pieces of prior art. Neology appeals. We affirm on the written-description ground and do not reach anticipation or obviousness.

I

A

Neology filed applications for both the '044 and '436 patents in 2012, both applications tracing by the same chain of continuation applications to an application filed in 2003 and a provisional application filed in 2002. The claims that appeared in the 2012 applications as filed (the 2012 claims) issued with very few changes as the claims in the '044 and

'436 patents. *Compare* J.A. 3549–54, *with* '044 patent, col. 23, line 5, through col. 24, line 63; *compare* J.A. 3755–59, *with* '436 patent, col. 23, line 13, through col. 25, line 17. The patents share a title, "System and Method for Providing Secure Identification Solutions," as well as a specification. They describe and claim methods and systems "for verifying and tracking identification information" in a secure system that, for one embodiment, "includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader/writer." *See*, *e.g.*, '044 patent, col. 1, lines 39–45. An example is an RF device (corresponding to the claims "RFID transponder") on an automobile, with identifying information embedded in the RFID device readable by an RFID reader. The important claim limitation for the asserted claims here involves exchanges of a "security key" between the RFID reader and transponder.

The claims of the '044 patent now at issue are claims 13, 14, and 25. Claims 13 and 14 depend on claim 10, which reads:

> 10. A toll system, comprising:
>
> a central database configured to:
>
> store toll accounts,
>
> receive identifiers related to toll accounts, and
>
> compare the received identifiers to identifiers associated with the toll accounts to determine if a match exists;
>
> an RFID reader comprising a radio and an antenna, the RFID reader configured to:
>
> send a first communication to a RFID transponder that includes a memory the contents of which include an identifier,

> send a second communication to the RFID transponder that includes a security key for validation by the RFID transponder,
>
> receive at least the identifier included in the memory contents in response to the second communication and as a result of validation of the security key, and transmit the identifier to the central database.

Id., col. 23, lines 39–56. Claim 13 adds the limitation of an RFID reader sending a "third communication . . . that includes a second security key for validation by the RFID transponder and receive further memory contents in response to the third communication and as a result of validation of the second security key." *Id.*, col. 23, line 64, through col. 24, line 4. Claim 14, which depends on claim 13, further requires that "the second security key is based on information received from the RFID transponder." *Id.*, col. 24, lines 5–7. Claim 25 depends on claim 23, which recites the same series of communications and transfers of security keys but for an RFID transponder, not the "toll system" of claim 10. *Id.*, col. 24, lines 37–50, 54–60.

The '436 patent claims also include the same series of communications between the RFID reader and transponder. '436 patent, col. 23, lines 13–43. Independent claim 1 recites:

> 1. A RFID reader, comprising:
>
> a radio and an antenna;
>
> a processor coupled with the radio, the processor configured to:
>
> send a first communication to a RFID transponder via the radio and the antenna that includes a memory the contents of which includes an identifier,

> send a second communication to the RFID transponder via the radio and the antenna that includes a security key for validation by the RFID transponder,
>
> receive at least the identifier included in the memory contents via the radio and the antenna in response to the second communication and as a result of validation of the security key, and
>
> transmit the identifier to a central database;
>
> wherein the processor is further configured to send a third communication to the RFID transponder via the radio and the antenna that includes a second security key for validation by the RFID transponder and receive via the radio and the antenna further memory contents in response to the third communication and as a result of validation of the second security key.

Id., col. 23, lines 13–34. Claims 2 and 4 depend directly on claim 1. Claim 2 adds the limitation that "the security key is based on information received from the RFID transponder." *Id.*, col. 23, lines 35–36. Claim 4 adds the limitation that "the second security key is based on information received from the RFID transponder." *Id.*, col. 23, lines 41–43.

B

Neology filed a complaint with the Commission on December 4, 2015. The complaint alleged infringement of various claims of the '044 and '436 patents, as well as claims of another patent not at issue here. Neology accused Kapsch TrafficCom U.S. Corp., Kapsch TrafficCom IVHS Technologies Holding Corp., Kapsch TrafficCom IVHS Holding Corp., Kapsch TrafficCom IVHS, Inc., Kapsch TrafficCom Canada Inc., Kapsch TrafficCom Holding Corp., Star Systems International, Ltd., and STAR RFID Co., Ltd. (collectively, Kapsch) of importing infringing products. 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.