Trials@uspto.gov
571.272.7822

Paper No. 12
Filed: June 4, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AXIS COMMUNICATIONS AB, CANON INC.,
and CANON U.S.A., INC.,
Petitioner,

v.

AVIGILON FORTRESS CORPORATION,
Patent Owner.

Case IPR2019-00236
Patent 7,868,912 B2 & C1

Before GEORGIANNA W. BRADEN, KIMBERLY McGRAW, and JESSICA C. KAISER, *Administrative Patent Judges*.

McGRAW, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 325(d) and 37 C.F.R. § 42.108

I. INTRODUCTION

Axis Communications AB, Canon Inc., and Canon U.S.A., Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of all claims (i.e., claims 1–4 and 6–36)[1] of U.S. Patent No. 7,868,912 B2 & C1 (Ex. 1001, "the '912 patent"). *See* 35 U.S.C. § 311. Patent Owner, Avigilon Fortress Corporation ("Patent Owner") filed a Preliminary Response. (Paper 8, "PO Resp."). Institution of an *inter partes* review is authorized by statute when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). Upon consideration of the Petition and Preliminary Response, we decline to institute review of claims 1–4 and 6–36 of the '912 patent.

A. Related Proceedings

Concurrent with the instant Petition, Petitioner filed another petition for *inter partes* review of the '912 patent as well as two separate petitions for *inter partes* review of related U.S. Patent No. 7,932,923. *See* Pet. 69; *Canon Inc. et al. v. Avigilon Fortress Corp.*, Case IPR2019-00235 (PTAB Nov. 12, 2018) (Paper 1); *Canon Inc. et al. v. Avigilon Fortress Corp.*, Case IPR2019-00311 (PTAB Nov. 12, 2018) (Paper 1); *Canon Inc. et al. v. Avigilon Fortress Corp.*, Case PR2019-00314 (PTAB Nov. 12, 2018) (Paper 1). Additionally, we instituted two *inter partes* review proceedings of related U.S. Patent No. 8,564,661. *See* Pet. 69; *Canon Inc. et al. v. Avigilon Fortress Corp.*, Case IPR2018-00138 (PTAB June 1, 2018) (Paper

[1] Claim 5 was canceled during reexamination. Ex. 1001, Reexamination Certificate, 1:19.

8); *Canon Inc. et al. v. Avigilon Fortress Corp.*, Case IPR2018-00140 (PTAB June 1, 2018) (Paper 8).

B. The '912 Patent

In general, the '912 patent, titled "Video Surveillance System Employing Video Primitives," is directed to an automatic video surveillance system. Ex. 1001, [54], 1:18–19. One object of the invention is to reduce the amount of video surveillance data needed to analyze the video. *See id.* at 2:42–44. Another object is to filter the data to identify desired portions of the data. *See id.* at 2:45–46. The '912 patent states the system can process video data in real-time and store "extracted video primitives" to allow high speed forensic event detection later. *Id.* at 5:16–19. Video primitives can include "observable attributes" of an object in a video feed, such as the size, shape, position, speed, color, and texture of the object, or scene descriptors, that describe the overall scene, such the location of sky or foliage, weather conditions, and lighting changes. *See id.* at 13:14–64.

Figure 2, shown below, is a flow diagram for an embodiment of the video surveillance system that involves setting up, calibrating, tasking, and operating the system. *See id.* at 4:26–27, Fig. 2.

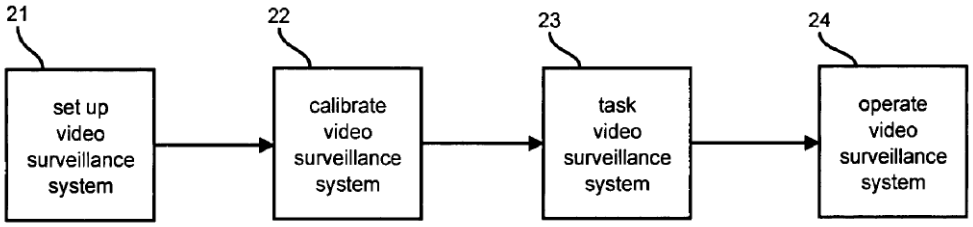

FIG. 2

As shown in the flow diagram of Figure 2 above, the video surveillance system includes tasking the surveillance system (block 23), which "involves specifying one or more event discriminators." *Id.* at 12:39–

44. "Event discriminators are identified with one or more objects (whose descriptions are based on video primitives), along with one or more special or temporal attributes. *Id.* at 5:29–33. For example, an operator can define an event discriminator (such as a "'loitering' event") as a "person" object in the "automatic teller machine" space for "longer than 15 minutes" and "between 10:00 p.m. and 6:00 a.m." *Id.* at 5:33–37.

Figure 3, reproduced below, is a flow diagram for tasking the video surveillance system. *Id.* at 4:30–31.

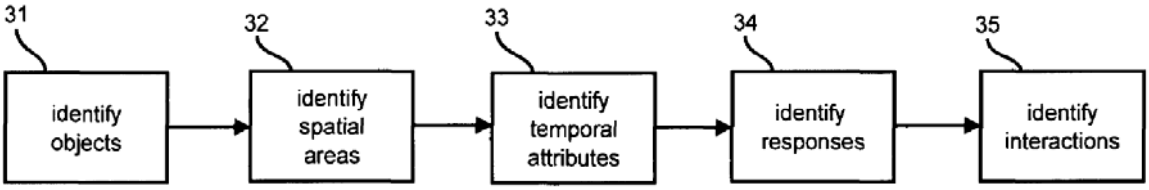

FIG. 3

As shown in the flow diagram of Figure 3, reproduced above, one step in tasking the video surveillance system is to identify responses (block 34). Examples of responses include activating an alarm, locking a door, *forwarding data such as video primitives to another computer system*, saving data to a computer-readable medium, as well as "*tasking the computer system . . . and/or another computer system*." *Id.* at 15:36–48 (emphasis added).

A flow diagram for operating one embodiment of the video surveillance system of the '912 patent is shown in Figure 4, reproduced below. *Id.* at 4:30–31.

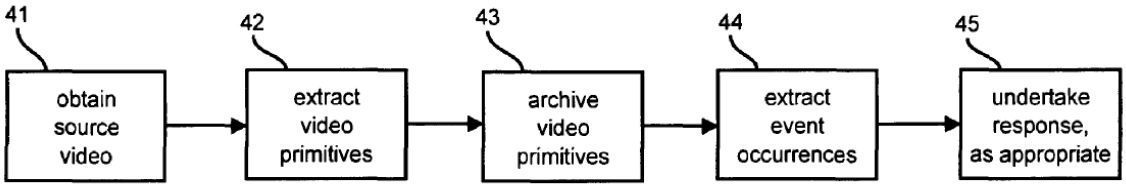

FIG. 4

As shown in Figure 4 above, the system extracts video primitives from a video (block 42), archives the video primitives (block 43), extracts event occurrences (block 44), and undertakes a response (block 45). *See also id.* at 20:36–38 (stating "video primitives are determined in block 42, and the event discriminators are determined from tasking the system in block 23 [of Figure 2]"). The '912 patent explains that in "block 44, event occurrences are extracted from the video primitives using event discriminators." *Id.* at 20:35–36. The event discriminators are used to filter the video primitives to determine if any event occurrences occurred. *Id.* at 20:39–41. For example, an event discriminator can look for a "wrong way" event as defined by a person traveling the "wrong way" into an area between 9:00 a.m. and 5:00 p.m. *Id.* at 20:41–43. "The event discriminators may also use other types of primitives . . . to detect occurrences." *Id.* at 20:49–51. The archiving step (block 43) of Figure 4 "is optional; if the system is to be used only in real-time, the archiving step can be skipped." *Id.* at 20:32–34. In "block 45, action is taken for each event occurrence extracted in block 44, as appropriate." *Id.* at 20:52–54.

Another embodiment is shown in Figure 9, reproduced below, in which the system analyses "archived video primitives with event discriminators to generate additional responses, for example, without needing to review the entire source video." *Id.* at 24:35–39.

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.