UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FITBIT, INC.,
Petitioner

v.

PHILIPS NORTH AMERICA LLC
Patent Owner

IPR2020-00783[1]
Patent No. 7,088,233

PETITIONER'S REPLY TO
PATENT OWNER'S RESPONSE

---

[1] Garmin International, Inc. Garmin USA, Inc., and Garmin Ltd., who filed a petition in IPR2020-00910, has been joined as a petitioner in this proceeding.

I. INTRODUCTION

Patent Owner's Response ("POR") relies on claim interpretations that improperly import limitations into the claims and inconsistent treatment of the prior art. Patent Owner's ("PO") arguments do not rebut the evidence demonstrating unpatentability explained in the Petition.

II. CLAIM CONSTRUCTION

A. "security mechanism governing information transmitted between the first personal device and the second device"

1. Board's construction is correct

Petitioner agrees there is "no need to construe [this] phrase[.]" (Paper 12 ("ID"), 15.) With ordinary language, the phrase describes what the "security mechanism" does and where it is located. The asserted prior art discloses this limitation under any reasonable interpretation. (*E.g.,* Paper 1 ("Petition"), 20-21, 36-38, 59-60.) Construction of this term is not "necessary to resolve the underlying controversy." *Toyota Motor Corp. v. Cellport Sys., Inc.*, IPR2015-00633, Paper No. 11 at 16 (Aug. 14, 2015); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

As the Board noted, "the use of passwords or encryption" in the '233 patent "can be used to secure information transmitted between personal device 100 and other points on the network." (ID, 14-15 (citing Ex.1001, 8:12–22, 13:25–67).) In fact, use of security keys, authorization, and encryption by the claimed "security

mechanism" is recited by dependent claims. (Ex.1001, claims 2-4; *id.*, 8:12-22 (password/security code).)

2. PO's construction is unsupported by evidence

PO's views of "security mechanism" and its alleged distinction from the prior art are premised on the testimony of its expert, Dr. Martin. (POR, 8-11, citing Ex.2026.) Highlighted by his cross-examination testimony, Dr. Martin on one hand confirms he is interpreting the term under its ordinary meaning by a POSITA at the relevant timeframe—not PO's proposed construction for the term (Ex.1076, 91:5-95:13; Ex.2026 ¶39)—yet on the other hand imports nebulous and shifting limitations into the term by opining that its purported ordinary meaning "depend[s] on what you're trying to protect against" in a particular application (Ex.1076, 95:14-96:5).

Dr. Martin's interpretation of the term is untethered from a POSITA's understanding in view of the specification at the patent's effective filing date, and instead applies an "ordinary meaning of security mechanism [that] depends on the threat you're trying to protect against" without reference to the specification or proper timeframe. (*See id.*, 96:7-99:5; *see also id.*, 63:6-64:25 (meaning "depend[s] upon the application that you're trying to do"), 126:20-129:17 ("security mechanism would depend upon those threats [you're trying to protect against]"), 138:19-140:15 ("depend[s] upon [] the alternative application area that you're contemplating"),

151:14-153:18, 65:15-67:5 (need to understand "what you're trying to protect against before you design the security mechanism").) Dr. Martin's conditional interpretation that relies on the subjective intended purpose of the mechanism is contrary to established claim construction principles, which further supports why PO's arguments should be rejected. *See Homeland Housewares, LLC v. Whirlpool Corp.*, 865 F.3d 1372, 1375-76 (Fed. Cir. 2017) (construction for "predetermined settling speed" that required the speed to be "determined for each use, depending on the particular blender or the individual contents of the blender" was "incorrect"); *Cochlear Bone Anchored Sols. AB v. Oticon Med. AB*, 958 F.3d 1348, 1356 (Fed. Cir. 2020) (rejecting notion claims required "particular intent or objective of a hearing-aid designer or manufacturer").

Moreover, even under his application-dependent interpretation, Dr. Martin opined that in certain applications, "encryption alone would satisfy the security mechanism of Claim 1." (*See* Ex.1076, 153:20-158:19 (if "only thing you're trying to protect against [is] eavesdropping of the transmissions by random passerby[s] ... and you're just trying to give your location to [] two other devices, then encryption would prevent the eavesdropping"), *see also id.*, 68:19-69:17, 131:11-132:11, 126:20-128:15 (same for "security keys"); Ex.2025, 132:25-133:4, Ex.2023, 13-15, POR 11.) Dr. Martin also conceded in other applications, multiple embodiments of security and "multiple levels of access would not necessarily be required. (Ex.1076,

150:2-153:18; *id.*, 129:19-132:19, 67:7-70:15 (similar); *see* Ex.1001, 13:41-54.) Dr. Martin's testimony undermines PO's reliance on Dr. Martin to contend that encryption cannot ever "govern or control [information] transmission." (POR, 10 (citing Ex.2007, ¶33).)

Despite attempts to sometimes import "multiple levels of authorization" into the "security mechanism," Dr. Martin also admitted that "multiple levels" of authorization "could encompass having full access and no access to a device"—"you either have access or you don't ... that's multiple levels." (Ex.1076, 62:8-63:4.) A security mechanism which provides full or no access to a device is disclosed by the prior art. (Pet., 36-38, 59-60, 66-70.)

3. PO's attempts to distinguish prior art are unsupported

PO attempts to distinguish "encryption of the *contents* of the signal" from "encryption of signals." (POR, 11.) But the specification does not distinguish between encryption of a signal and encryption of the signal contents. Instead, the specification and claims expressly include "encryption" within the scope of the "security mechanism." (Ex.1001, 13:41-46, claim 2.) PO appears to infer its distinction from Figure 5 and its expert's opinions. (POR, 10-11.) But PO and Dr. Martin concede that Figure 5 is but one exemplary "embodiment" (POR, 10; Ex.1001, 11:46-49, 13:31-32) and "claim 1 is not limited to that" (Ex.1076, 83:20-84:4; *id.*, 60:2-19, 114:2-23).

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.