UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PANASONIC CORPORATION OF NORTH AMERICA *et al*.,
Petitioner

vs.

CELLSPIN SOFT, INC.,
Patent Owner

Case IPR2019-00131
Patent No. 9,258,698

# PATENT OWNER'S OBJECTIONS TO PETITIONERS' REPLY AND TO EVIDENCE SUBMITTED WITH PETITIONERS' REPLY

Including pursuant to 37 C.F.R. §§ 42.23 and 42.64, Patent Owner hereby objects to the following issues and  matters, including theories, arguments and evidence included in and with Petitioners' Reply filed on October 15, 2019.  These objections are timely filed, including pursuant to 37 C.F.R. § 42.64.

| **Page or Exhibit** | **Material objected to** | **Objections** |
|---|---|---|
| Strawn[1] p. 4 | 10.  ... Furthermore, it is my opinion that a person of ordinary skill in the art would have had many reasons to combine, supplement, and/or modify the teachings of Mashita, Onishi, and Hiraishi to create the systems claimed in the Challenged Claims. Additionally, because the combination of Mashita, Onishi, and Hiraishi to create the systems claimed in the Challenged Claims involves using well-known components and technologies, according to their established functions, with only minor modifications, a POSITA would have reasonably expected success. Accordingly, the Challenged Claims would have been obvious in view of Mashita, Onishi, and Hiraishi. | Improper new evidence, a new direction/theory/argument/ approach/issue for reply, including under 37 CFR § 42.23, including because it does not only or properly respond to arguments raised in Cellspin's opposition, but rather it belatedly raises new directions/theories/arguments/ approaches/issues that could have been raised in the Petition and should not be considered in a reply. Without limitation, this attempt at a new, catch-all theory for obviousness (including that lacks any substance and is, at most, wholly conclusory), as well as the other new matters in the quoted text at left, is new and improper on reply. Cellspin further objects to those portions of the reply that rely upon these materials from the Second Strawn Declaration, including for the same reasons. |
| Strawn pp. 5-8 | 13.  … Furthermore, I based my understanding on the definition of "paired device" in the Bluetooth Specification: "A Bluetooth device with which a link key has been exchanged (either before connection establishment was requested or during connecting phase." [Exhibit 2018, p. 92]. This definition, coupled with the overall description of pairing in the Bluetooth Specification, means that if a PIN has been successfully entered (for example by matching PIN codes), as Mashita discloses, then Bluetooth pairing occurs. I used this definition of "pairing" when I was analyzing | Improper new evidence, a new direction/theory/argument/ approach/issue for reply, including under 37 CFR § 42.23, including because it does not only or properly respond to arguments raised in Cellspin's opposition, but rather it belatedly raises new directions/theories/arguments/ approaches/issues that could have been raised in the Petition and should not be considered in a reply. Without limitation, this new attempt to assert that the entering of the |

[1] "Strawn" refers to the Second Strawn Declaration at Exh. 1024.

| Page or Exhibit | Material objected to | Objections |
|---|---|---|
| | Mashita.<br>13. My understanding is confirmed for example in the Bluetooth Specification [Exhibit 2018, pp. 865-867; Figure 3.1, reproduced also Foley Declaration, ¶1011]. According to the Bluetooth Specification, if a PIN has been input to both devices, and the connection is successful (by matching the PIN codes), pairing has happened.<br>14. … The fact remains that Bluetooth pairing necessarily occurs in order for these subsequent steps to occur, contrary to the Foley Declaration.<br>15. The PIN, entered by the user during Bluetooth pairing, is combined with the Bluetooth Device Address BD_ADDR during authentication, generating an “initialization key:” “When the initialization key is generated, the PIN is augmented with the BD_ADDR.” [Exhibit 2018, p. 1032]. The initialization key is then used to create a link key: “When both devices have calculated Kinit [the initialization key] the link key shall be created, and a mutual authentication is performed.” [Exhibit 2018, p. 412 (emphasis added)]. The link key is generated using an algorithm called E22, with the PIN and BD_ADDR as inputs [ibid., p. 1032; pp. 1055-1057]. The output of algorithm E22 is the 128-bit link key [ibid., p. 1055]. For authentication, the link key is involved: “The link key itself is used in the authentication routine.” [ibid., p. 1029]. As the Bluetooth Specification states, the “key generating algorithm” exploits a “cryptographic function.” [ibid., p. 1056].<br>16. As I outlined in the Strawn Declaration [¶83], this is exactly what happens in Mashita. The BD_ADDR of the Bluetooth Specification is the “physical address” of Mashita cited in the Strawn Declaration. The PIN of the Bluetooth Specification is the PIN of Mashita, and that PIN is used during Bluetooth pairing. | Mashita PIN results in Bluetooth pairing, that Mashita’s PIN exchange comprises Bluetooth pairing, that the Mashita PIN is a Bluetooth PIN, that the Bluetooth specification supports the Mashita PIN resulting in pairing and/or a link key; that a Mashita PIN is sufficient for pairing, and/or that the Mashita PIN is used for a link key, as well as the other new matters in the quoted text at left, is new, could have been raised in the Petition and is improper on reply. Further, without limitation, Dr. Strawn and Petitioners’ original theory was that Mashita’s PIN exchange resulted in pairing in and of itself and without parallels, analogies or other links being made to specific Bluetooth methods. Without limitation, the discussion of Bluetooth, PINs, pairing, keys, algorithms and/or encryption at left is a new and improper direction/theory/argument/approach/issue that is improper on reply. Cellspin further objects to those portions of the reply that rely upon these materials from the Second Strawn Declaration, including for the same reasons. |

| Page or Exhibit | Material objected to | Objections |
|---|---|---|
| | Authentication in Bluetooth [e.g., Exhibit 2018, p. 1048 et seq.] is the “connection authentication” of Mashita [Strawn Declaration, ¶85].<br>17. … To clarify, pairing explicitly happens if a PIN is exchanged, as in Mashita, and the link key required for authentication is then calculated from the PIN. Furthermore, if pairing happened previously and a link key derived from the PIN already exists, then the link key is simply provided and pairing need not be repeated this time.<br>18. The Bluetooth Specification further clarifies that the use of PIN input confirms that pairing has happened. As I noted above, Mashita discloses that “an identical Personal Identification Number (PIN) code is input to both the cellular phone 102 and the digital camera 101.” [Mashita, 0051]. Step 7a discussed above is shown in more detail in another illustration in the Bluetooth Specification, in which the PIN input step is shown explicitly for both devices as “User Inputs PIN Code” [Exhibit 2018, p. 866], as disclosed in Mashita. The expanded illustration makes it clear that if a PIN is input by a user, the devices are performing “Step 7a: Pairing during connection establishment” in the words of the caption to the illustration [ibid., p. 866]. Although this discussion refers to Version 2.1 + EDR, earlier versions of the Bluetooth Specification documents also described using a PIN input to establish a paired connection. I discussed this in Strawn Declaration with reference to Version 2.0 + EDR. [Ex. 1001, ¶87, citing Ex. 1017, p. 251]. In addition, the Bluetooth Specification notes that using a 4-digit PIN for pairing was common for devices compliant with both Version 2.0 + EDR “and earlier versions.” [Ex. 2018, p. 131]. | |
| Strawn pp. 9-10 | 20. … Because Mashita discloses that a PIN is “input to both the cellular phone 102 | Improper new evidence, a new direction/theory/argument/approach/ |

| Page or Exhibit | Material objected to | Objections |
|---|---|---|
| | and the digital camera 101," with both being Bluetooth devices, and because Mashita then discloses "an authentication process for local wireless connection," a POSITA would understand that Mashita clearly discloses that Bluetooth pairing has in fact occurred, as I outlined above.<br>21. … Mashita does not need to recite the details of every single step in the Bluetooth Specification in order for POSITA to understand that a link key is calculated, derived from the PIN…<br>22. It is important to distinguish between what happens in Bluetooth with the PIN during pairing and authentication, and what happens later when data is to be encrypted. The user input of a PIN generates a link key, as described above, which can be further incorporated into a later step in which actual data transferred between the camera and cellular phone, such as image data, is encrypted. This is the separate step 8 in the illustration (Exhibit 2018, Figure 3.1) reproduced in the Foley Declaration [¶101]. Encrypted communication in this sense can only follow authentication which, as I have shown, requires pairing: "If at least one authentication has been performed encryption may be used." [Exhibit 2018, p. 418]. As I discussed, the PIN is used to derive the authentication key, which in turn is used to derive an encryption key for data exchange: "The encryption key is derived from the authentication key [i.e., link key] during the authentication process." [Exhibit 2018, p. 1025, see also p. 1026 (noting that the authentication key "is often referred to as the link key"), p. 1034]. The Challenged Claims do not require encryption of data passed between camera and cellular phone, such as image data. Even if there were such a data encryption requirement, a POSITA would understand that the PIN, device address, pairing, and authentication disclosed in | issue for reply, including under 37 CFR § 42.23, including because it does not only or properly respond to arguments raised in Cellspin's opposition, but rather it belatedly raises new directions/theories/arguments/ approaches/issues that could have been raised in the Petition and should not be considered in a reply. Without limitation, this new attempt to assert that Mashita discloses Bluetooth pairing, a link key is calculated/derived from the Mashita PIN, that Mashita discloses encryption including encryption/link keys and/or that Mashita's authentication results in encryption, that "the PIN, device address, pairing, and authentication disclosed in Mashita provide the prerequisites for such data encryption in Bluetooth as well as the other new matters in the quoted text at left, is new and improper on reply. Further, without limitation, Dr. Strawn and Petitioners' original theory was that Mashita's PIN exchange resulted in pairing in and of itself and without parallels, analogies or other links being made to specific Bluetooth methods, and that the alleged encryption of Mashita consisted of the PIN being secret. Without limitation, all of the discussion of Bluetooth, PINs, pairing, keys and encryption at left belatedly raises new directions/theories/arguments/ approaches/issues that are improper on reply. Cellspin further objects to those portions of the reply that rely upon these materials from the Second Strawn Declaration, including for the same reasons. |

# 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.

**WHAT WILL YOU BUILD?** | **sales@docketalarm.com** | **1-866-77-FASTCASE**

Smarter legal research.