

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

TCL INDUSTRIES HOLDINGS CO., LTD.,  
Petitioner,

v.

KONINKLIJKE PHILIPS N.V.,  
Patent Owner.

---

IPR2021-00547  
Patent 9,590,977 B2

---

Before KEVIN F. TURNER, STACEY G. WHITE, and  
RUSSELL E. CASS, *Administrative Patent Judges*.

CASS, *Administrative Patent Judge*.

DECISION

Denying Petitioner's Request for Rehearing of Decision Denying Institution  
of *Inter Partes* Review  
*37 C.F.R. § 42.71(d)*

## I. INTRODUCTION

### A. Background

Petitioner TCL Industries Holdings Co., Ltd. (“Petitioner”) filed a Request for Rehearing under 37 C.F.R. § 42.71(d) (Paper 11 (“Req. Reh’g)). Petitioner’s Request for Rehearing seeks reconsideration of our Decision Denying Institution of *Inter Partes* Review of U.S. Patent No. 9,590,977 B2 (Ex. 1001, “the ’977 patent”). Paper 10 (“Dec.”). For the reasons set forth below, Petitioner’s Request is *denied*.

## II. BACKGROUND

Petitioner filed a Petition requesting *inter parties* review of claims 22–31 (the “challenged claims”) of the ’977 patent. Paper 1 (“Pet.”). The Petition asserted that independent claim 22 is unpatentable over EP 1045585 A1 to Maillard et al. (Ex. 1004, “Maillard”), in view of WO 97/39553 A1 to Davis (Ex. 1005, “Davis”) and WO 02/35036 A1 to Lundkvist (Ex. 1006, “Lundkvist”). Pet. 1. In our Decision Denying Institution, we determined that Petitioner had failed to articulate sufficient reasoning for combining Maillard, Davis, and Lundkvist, and therefore, had not established a reasonable likelihood that claim 22 was unpatentable. Dec. 19–22. We also determined that Petitioner had failed to establish a reasonable likelihood that the remaining dependent claims were unpatentable. *Id.* at 22–23.

## III. STANDARD OF REVIEW

A party requesting rehearing bears the burden of showing that the decision should be modified, and “[t]he request must specifically identify all matters the party believes the Board misapprehended or overlooked.” 37 C.F.R. § 42.71(d). Institution of an *inter partes* review is authorized by statute only 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) (2018). When considering a request for rehearing of a decision whether to institute an *inter partes* review, the Board reviews its decision for an abuse of discretion. 37 C.F.R. § 42.71(c). An abuse of discretion occurs when a “decision [i]s based on an erroneous conclusion of law or clearly erroneous factual findings, or . . . a clear error of judgment.” *PPG Indus. Inc. v. Celanese Polymer Specialties Co.*, 840 F.2d 1565, 1567 (Fed. Cir. 1988). “It is not an abuse of discretion to have made an analysis or conclusion with which a party disagrees,” and “mere disagreement with the Board’s analysis or conclusion is not a proper basis for rehearing.” *EMC Corp. v. PersonalWeb Techs., LLC*, IPR2013-00085, Paper 29 at 4 (PTAB June 5, 2013).

#### IV. ANALYSIS

In its Request for Rehearing, Petitioner makes two arguments. First, Petitioner argues that the Petition identified sufficient rationale to combine based on Davis’s teaching to use proximity awareness in smart card systems. Req. Reh’g 2. Second, Petitioner argues that the Petition identified sufficient rationale to combine based on risk of unauthorized redistribution outside the authorized local network. *Id.* at 9. We address these arguments in turn below.

##### *A. Motivation to Combine Based on Davis’s Teaching to Use Proximity Awareness in Smart Card Systems*

In the Petition, Petitioner argued that one of ordinary skill would have been motivated to combine Maillard and Davis because Davis recognizes the vulnerability of smartcard systems when a “user leaves accesses his or her personal computer and leaves the personal computer unattended for some duration without removing the card or disabling the personal computer

during his or her absence,” thereby leaving the personal computer exposed to access by unauthorized users. Pet. 31 (quoting Ex. 1005, 2:28–3:19). In our Decision, we determined that Petitioner’s articulated rationale failed to sufficiently explain why this problem would apply to Maillard’s system. Dec. 19–20. In particular, we explained that the record did not sufficiently show why in Maillard’s system it would have been a problem for the user to leave the security module unattended while connected to the DVD player. *Id.*

Petitioner contends that we misapprehended or misevaluated its rationale to combine because Davis is not limited to a user accessing a computer, but rather “teaches that its technique is an improvement for *any* electronic device that uses a smart card for secure access, which Maillard’s DVD player does.” Req. Reh’g 6–7. Additionally, Petitioner contends that Maillard is not limited to a DVD player application but rather “discloses that its techniques are relevant to the communication of protected content between various types of devices,” including “software content on a hard disk of a computer.” *Id.* at 7. “Hence,” Petitioner argues, “while the rationale to combine disclosed in Davis and relied on in the Petition is itself sufficient to demonstrate a rationale to modify the DVD player embodiment in Maillard, the rationale to combine is further supported for Maillard’s broader disclosure of other electronic devices.” *Id.* at 8.

We are not persuaded by Petitioner’s arguments. Although Petitioner now argues that Davis is applicable to any electronic device, Petitioner did not make that argument in the Petition, but rather relied on Davis’s teaching that smart card systems “can be vulnerable when ‘the user accesses his or her personal computer and leaves the personal computer unattended for

some duration without removing the card or disabling the personal computer during his or her absence.” Pet. 31 (quoting Ex. 1005, 2:28–3:19). Indeed, the portions of the Petition that the Request for Rehearing points to as making this argument (*Id.* at 12:17–13:1, 26:4–10) are taken from the background sections describing the state of the prior art and the Davis reference, not from the section arguing that it would have been obvious to combine the references (*Id.* 30–33). Similarly, Petitioner’s argument that Maillard could be combined with Davis because Maillard’s technique is relevant to other electronic devices, including software content on a computer hard disk, was not made in the Petition. *See id.* at 30–33. We cannot have misapprehended or overlooked points and arguments that Petitioner never made in the Petition.

Moreover, even if we consider these newly-raised arguments, Petitioner’s evidence still falls short. The quoted portion of Davis extends its teachings to “a peripheral to the computer (printer, mass storage device, etc.), door locking mechanisms (i.e., garage door opener, electronic door locks) and the like.” Ex. 1005, 7:13–19, *quoted in* Req. Reh’g 6–7. These are all situations, like the computer in Davis’s preferred embodiment, where the device being protected is in a location where it is exposed to many people who might not be authorized to access it, leaving it vulnerable when a user accesses the device and then leaves it unattended for a period of time. *See* Ex. 1005, 2:28–3:19. In this situation, Davis’s proximity measurement prevents access by such unauthorized persons by restricting access to an authorized user who is in close physical proximity to the device. Maillard, on the other hand, has a different purpose, namely “provid[ing] secure communication of data between devices” in a digital audiovisual system “to

prevent the unauthorized copying and distribution of digitally recorded data.” Ex. 1004 ¶ 78. Maillard says nothing about preventing unauthorized users from accessing a device after the authorized user accesses it and leaves it unattended, which is the purpose of Davis’s proximity detection. Thus, Petitioner fails to adequately show why one of ordinary skill would have applied Davis’s teaching to Maillard’s system, which has a different context and purpose.

Petitioner’s argument that Maillard includes a “broader disclosure of other electronic devices” besides a DVD player is also unavailing. The pertinent portion of Maillard states that the invention also may be applied “to the playing of exclusive audio information subsequently recorded on a DAT or minidisc recorder or even to the communication of software recorded on the hard disc of a computer.” Ex. 1004 ¶ 74. Like the DVD player preferred embodiment, these are all examples of providing secure communication between two devices physically connected together to prevent unauthorized copying and distribution. Petitioner fails to adequately show why one of ordinary skill would have found Davis’s token and proximity detection to be useful in these alternative embodiments of Maillard’s system.

*B. Motivation to Combine Based on the Risk of Unauthorized Redistribution Outside the Authorized Local Network*

In the Petition, Petitioner argued that one of ordinary skill would have “recognized that Maillard’s technique, which was described using an example home network using IEEE 1394 communication link . . . could be susceptible to attacks that would allow devices outside of the home network to infiltrate the home network.” Pet. 31 (citing Ex. 1004 ¶¶ 53, 58; Ex. 1003 ¶¶ 138–142 (Nielson declaration)).

In our Institution Decision, we determined that this argument lacked sufficient evidentiary support. Dec. 20–22. We noted that Petitioner did not point to any statements in the prior art suggesting that the risk of an unauthorized person breaking into a system such as Maillard’s would have been recognized as a problem by one of ordinary skill. *Id.* at 21 (citing Pet. 31–32; Ex. 1003 ¶¶ 131–135). We also explained that Dr. Nielson failed to provide evidence to support his assertions that “[i]t was known to a POSITA that data signals of one communication type, such as IEEE 1394 as mentioned in Maillard, can be vulnerable to attacks, where signals could be adapted and retransmitted over more traditionally long distance mechanisms, such as Ethernet,” or (2) “[a] POSITA would readily comprehend that Maillard’s security module for device authorization and authentication in a home network could be exfiltrated to a remote location.” *Id.* (citing Pet. 30–33, 56–61; Ex. 1003 ¶¶ 131–141 (alterations in original)).

We further noted in our Institution Decision that Patent Owner had introduced evidence that an “IEEE bus link” would have been understood to be a physical cable that connects two devices together. Dec. 21–22 (citing Ex. 1004 ¶ 53; Ex. 2001, 94). We agreed with Patent Owner that the Petition did not sufficiently explain why adding a distance measurement between Maillard’s security module and one of the other devices would enhance security. *Id.* at 22.

In its Request for Rehearing, Petitioner argues that we misapprehended Dr. Nielson’s explanation because we made an improper assumption that “unauthorized distribution can only occur due to external actors.” Req. Reh’g 12. Petitioner asserts that “[u]nauthorized distribution could just as easily be performed by a user *in the home* transmitting the

content outside the home network without authorization,” but “because Maillard’s system is not able to determine whether the target device is actually in the home network, ‘Maillard’s security module would enable the DVD player to transmit to another authorized TV anywhere in the world so long as the security module is connected in this way.’” *Id.* at 12–13 (citing Ex. 1003 ¶ 141).

We are not persuaded by Petitioner’s argument on rehearing. The Petition merely asserted that one of ordinary skill would have recognized that Maillard’s technique “could be susceptible to attacks that would allow *devices outside of the home network to infiltrate* the home network,” and thus, argued that it would have been obvious to use Davis’s proximity detection. Pet. 31 (emphasis added). The Petition did not assert that the risk of a person *inside the home* transmitting protected content from a DVD to an outside location without authorization would have provided motivation to add Davis’s proximity detection to Maillard. *Id.* at 31–32.

Additionally, Petitioner does not provide any more evidentiary support that one of ordinary skill would have recognized the risk of unauthorized transmission from a person *inside the home* to an external location than it does that one of ordinary skill would have recognized the risk of unauthorized transition due to an *external actor* infiltrating the system. In this regard, neither Petitioner nor Dr. Nielson point to any statements in Maillard, Davis, Lundkvist, or any other reference in the record indicating that one of ordinary skill would have recognized this risk of unauthorized transmission from a person inside the home as a problem with the Maillard system. Moreover, as we explained in the Institution Decision, Patent Owner introduces evidence that the IEEE 1394 bus link



described in Maillard, was a physical cable connecting two devices together (Pet. 21 (citing Ex. 1004 ¶ 53; Ex. 2001, 94)), and Petitioner does not sufficiently explain why, when the devices are physically connected, adding a distance measurement between the security module and one of the other devices would enhance security.

Furthermore, even if one of ordinary skill had recognized the risk that a person inside the home could make an unauthorized transmission to a TV outside the home, neither Petitioner nor Dr. Nielson sufficiently show why one of ordinary skill in the art would have been motivated to look to Davis's proximity-aware technique to solve this problem. As discussed above, Davis uses proximity of the user to the computer for authentication because the computer is in a location (such as a business) that is accessible to multiple unauthorized users. *See* Ex. 1005, 2:28–3:19. Maillard's DVD player, by contrast, is located in the home and, presumably, not readily accessible by unauthorized users in the same manner as Davis's computer. Therefore, there is insufficient evidence in the present record that of ordinary skill would have looked to Davis's proximity authorization technique to improve security in Maillard's home DVD system.

## V. CONCLUSION

The Request for Rehearing does not demonstrate that the Institution Decision misapprehended or overlooked any matters, or that we abused our discretion in arriving at the conclusions set forth in the Decision.

## VI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Request for rehearing is *denied*.

IPR2021-00547  
Patent 9,590,977 B2

For PETITIONER:

Babak Tehranchi  
John Schnurer  
Bing Ai  
Kevin Patariu  
Yun Lu  
PERKINS COIE LLP  
tehranchi-ptab@perkinscoie.com  
schnurer-ptab@perkinscoie.com  
ai-ptab@perkinscoie.com  
patariu-ptab@perkinscoie.com  
lu-ptab@perkinscoie.com

For PATENT OWNER:

William Meunier  
Michael Renaud  
Derek Constantine  
MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C.  
wameunier@mintz.com  
mtrenaud@mintz.com  
deconstantine@mintz.com