

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TOYOTA MOTOR CORP.,
Petitioner,

v.

EMERGING AUTOMOTIVE LLC,
Patent Owner.

Case No. IPR2024-00814
U.S. Patent No. 11,396,244

**REPLY DECLARATION OF KEVIN C. ALMEROTH, PH.D.
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 11,396,244**

Table of Contents

I.	Introduction.....	3
II.	Qualifications and Background	4
III.	Materials Considered	4
IV.	Legal Standards	5
V.	<i>Rector's</i> Implementation and Enforcement of User Settings.....	5
VI.	<i>Kleve's</i> Additional Security	9
VII.	Conclusion	12

I. INTRODUCTION

1. I, Kevin C. Almeroth, Ph.D., submit this declaration to state my opinions on the matter described below.

2. I have been retained by Petitioner Toyota Motor Corp. (“Petitioner”), as an independent expert in this proceeding before the United States Patent and Trademark Office. Although I am being compensated at my usual and customary rate of \$800 per hour, no part of my compensation depends on the outcome of this proceeding, and I have no other interest in this proceeding.

3. I previously submitted a declaration (Ex. 1005) in support of Petitioner’s Petition in the proceeding.

4. I understand that this proceeding involves U.S. Patent No. 11,396,244 (the “’244 patent”) (Ex. 1001), assigned to Patent Owner Emerging Automotive LLC (“Patent Owner”), and I have been asked to provide my opinions as to the patentability of the claims of the ’244 patent.

5. I have been asked to consider and provide opinions regarding certain issues raised by Patent Owner in its Patent Owner Response.

6. Based on the prior art discussed in my prior declaration, it remains my opinion that all claims of the ’244 patent addressed in my original declaration are unpatentable for the reasons provided in my original declaration, and for the additional reasons provided below.

II. QUALIFICATIONS AND BACKGROUND

7. My prior declaration summarizes my qualifications and background.

III. MATERIALS CONSIDERED

8. In forming my opinions, I have reviewed the following documents:

Exhibit	Description
Ex. 1001	U.S. Patent No. 11,396,244 to Penilla et al. (“244 patent”)
Ex. 1002	Certified Prosecution File History for U.S. Patent No. 11,396,244
Ex. 1003	U.S. Provisional Application No. 61/745,729
Ex. 1006	U.S. Patent Application Pub. No. 2011/0137520 A1 to Jay Rector et al. (“ <i>Rector</i> ”)
Ex. 1007	U.S. Patent Application Pub. No. 2014/0129053 A1 to Robert Bruce Kleve et al. (“ <i>Kleve</i> ”)
Ex. 1008	U.S. Patent No. 6,505,780 B1 to Amr Yassin et al. (“ <i>Yassin</i> ”)
Ex. 1009	U.S. Patent Application Pub. No. 2006/0136106 A1 to Russell Patenaude et al. (“ <i>Patenaude</i> ”)
Ex. 1010	U.S. Patent Application Pub. No. 2011/0035031 A1 to Jens Faenger et al. (“ <i>Faenger</i> ”)
Ex. 1013	U.S. Provisional Application No. 61/478,436
Ex. 1014	As-filed specification of U.S. Application No. 13/452,881
Ex. 1015	As-filed specification of U.S. Application No. 13/842,158
Ex. 1033	OnStar Website, The Evolution of OnStar, https://www.onstar.com/why-onstar/evolution-of-onstar-innovations
Ex. 1034	OnStar Website, Stolen Chevrolet Cruze quickly recovered

	(Apr. 18, 2013) https://www.onstar.com/stories/onstar-helps-recover-stolen-car
Ex. 1035	Damon Lavrinc, <i>In Automotive First, Tesla Pushes Over-the-Air Software Patch</i> , Wired (Sep. 24, 2012) https://www.wired.com/2012/09/tesla-over-the-air/
Ex. 1036	Edmunds Website, Can Your Car Be Hacked? https://www.edmunds.com/car-technology/can-your-car-be-hacked.html
Ex. 2001	Declaration Of Dr. Sam Malek In Support Of Patent Owner's Preliminary Response
Ex. 2003	Declaration Of Dr. Sam Malek In Support Of Patent Owner's Response
Paper 1	Petition
Paper 6	Patent Owner's Preliminary Response
Paper 7	Petitioner's Pre-Institution Reply
Paper 9	Patent Owner's Sur-Reply
Paper 11	Institution Decision
Paper 16	Patent Owner's Response

IV. LEGAL STANDARDS

9. My prior declaration summarizes my understanding of the legal principles that guide my analysis to determine if the claims are unpatentable in light of the prior art.

V. RECTOR'S IMPLEMENTATION AND ENFORCEMENT OF USER SETTINGS

10. I understand that Patent Owner contends that the teachings of *Rector*

belong to two supposedly “distinct embodiments”— A “method of controlling a driver’s settings on a smart vehicle,” and a “system of controlling a driver’s settings.” POR, 22. Patent Owner’s expert, Dr. Malek, opines that Rector discloses “(1) *Rector*’s system for controlling a driver’s settings . . . which teaches that a server determines permitted settings,” and “(2) *Rector*’s method of controlling a driver’s settings on a smart vehicle . . . which directs that a smart vehicle determines the driver’s permitted settings.” Ex. 2003, ¶ 67. I disagree that a POSA would compartmentalize *Rector*’s disclosures in the manner Patent Owner and Dr. Malek suggest.

11. Dr. Malek suggests that the differentiating factor between “*Rector*’s system” and “*Rector*’s method” is the entity that determines the “permitted settings.” *Id.* According to Dr. Malek, *Rector*’s “method” teaches only local functionality. Ex. 2003, ¶ 66 (“a smart vehicle, not a server, executes the above-referenced steps of the method”). But the very paragraph that Dr. Malek defines as *Rector*’s “method” plainly recites:

Alternatively, the unique identifier may be compared with a set of unique identifiers **on a server on a network**. With the identity of the driver determined, the smart vehicle looks up settings for the driver S352. These settings may include driver created settings, controlling authority settings, etc. **The settings are determined by**

comparing the driver's identity with a database of identities with corresponding settings. This database may be on the network . . .

Rector, [0043] (emphasis added).

12. In fact, *Rector* discloses a “settings server” that “determine[s] the permitted settings for the user” and “transmit[s] the permitted settings to the [vehicle].” *Rector*, Claim 1; *see also* Petition, 27-28; Ex. 1005, ¶ 127. This “settings server” is discussed throughout *Rector*’s specification, from paragraph [0009] to paragraph [0057].

13. Specifically, *Rector*’s “server logic” existing on the “settings server” executes the step of “transmit[ting] the permitted settings to the [vehicle].” *Rector*, claim 1. *Rector* then describes “limit[ing] functions of the smart vehicle based upon the permitted settings.” *Id.* For example, *Rector*’s vehicle may implement “controlling authority settings” received from the settings server, such as a maximum speed using a speed governor. *Rector*, [0031]-[0032]. Further, “[w]ith the settings determined for the driver, the smart vehicle detects an attempted change of a setting.” *Rector*, [0043]. “The smart vehicle determines whether the attempted change of the setting is permitted,” and if it is, “the change is allowed.” *Id.*

14. In view of *Rector*’s many teachings regarding server-side

functionality, a POSA would not have compartmentalized *Rector*'s disclosures in such a way to exclude server-side functionality from *Rector*'s "method of controlling a driver's settings," which specifically teaches server-side functionality. Rather, *Rector*'s express disclosure of "alternatively" performing functions on a "server" and "database of a network" would have directed a POSA to teachings concerning *Rector*'s "settings server." A POSA would have understood that *Rector*'s "settings sever" is an example of the "server" described in paragraph [0043].

15. I also understand that Patent Owner disputes whether *Rector*'s "transmit[ting of] the permitted settings to the [vehicle]" causes the vehicle to implement those settings. Dr. Malek opines that "*Rector* does not use the word 'cause' . . . nor do [*Rector*'s] disclosures suggest that the system's server transmitting settings 'cause the client logic to implement them.'" Ex. 2003, 32. I disagree.

16. *Rector* plainly discloses "transmit[ting] the permitted settings to the client logic, wherein the client logic limits functions of the smart vehicle *based upon the permitted settings*." *Rector*, [0009] (emphasis added). It is the transmitting of the permitted settings that precipitates the "limit[ing]," i.e. setting, step. *Rector* does not disclose that the client logic on the vehicle can ignore the permitted settings received from the server; nor would a POSA expect this to be a

possibility.

VI. KLEVE'S ADDITIONAL SECURITY

17. In my first declaration, I opined that “[a] POSA would have been motivated and found it obvious to combine the teachings of *Rector* and *Kleve*, and would have done so for multiple reasons. For example, one would have considered the teachings of *Kleve* for improving the security of *Rector*, and would have had a reasonable expectation of success in doing so.” Ex. 1005, ¶ 114. I understand that Dr. Malek disputes my conclusion because, in his view, “[i]t is common knowledge in computer science that distributed software systems are less secure than local software systems.” Ex. 2003, ¶ 78. I disagree with Dr. Malek.

18. As I noted in my first declaration there are several situations in which server-side authentication could improve the security of Rector’s client-side verification. For example, “a server may be kept more up-to-date, and may be better protected from security attacks. For example, there may be a situation where a vehicle is in a location where it is unable to communicate with a centralized authority (like a server or data center that administers a settings-applying system). While it is out of contact, the vehicle would be unable to receive updates, such as changes to credentials, changes to who is authorized, or a user’s level of access. A user might have realized that his/her password is compromised and attempt to change it via other devices connected to the server. However, if the vehicle is out

of contact with the server it would not be able to update its registry of credentials, and if it uses only local verification, it would be vulnerable to login attempts using compromised credentials. The server-side verification may be done above and beyond any verification that takes place locally.” Ex. 1005, 62-63.

19. Dr. Malek does not address any of the specific motivations discussed above but rather presumes that “[c]omputer networks are the major source of security attacks.” Ex. 2003, 39. While I agree that computer networks, such as the internet, are the source of many security attacks, this does not indicate that a POSA would be lead away from implementing *Kleve*’s server-side verification. Ex. 1007, ¶ [0049].

20. A POSA would have recognized the tradeoffs associated with client-side and server-side verification. In my opinion, a POSA would recognize that any potential security-related disadvantages of implementing *Kleve*’s server-side verification would be outweighed by the advantages, including those I detailed in my first declaration. Further, I do not believe Dr. Malek’s generalized security concerns would lead a POSA away from utilizing *Kleve*’s server-side verification in the context of Rector’s invention, which also expressly teaches server-side functionality. In fact, based on my experience, around the time of the purported invention of the ’244 patent automakers were adding server-side functionality to vehicles, including remote recovery systems, like OnStar, and over-the-air,

internet-enabled updates for security patching. *See* Ex. 1033, 3 (describing “the industry’s first embedded telematics system” debuting in 1996); Ex. 1034 (example of OnStar telematics technology recovering a stolen vehicle in 2013); Ex. 1035, 1 (noting that Tesla was “Push[ing] Over-the-Air Software Patch[es]” in 2012); Ex. 1036, 1 (noting that “there's been only one incidence of car hacking” as of the article’s 2015 publishing), 2 (noting that “over-the-air (OTA) software updates can also be used to plug holes in the security of a connected car . . .”). Despite Dr. Malek’s concern regarding the security of “[c]omputer networks,” automakers nonetheless decided to implement this functionality which, in at least some circumstances, have rendered automobiles more secure. *Id.*

21. Further, Dr. Malek’s presumption is based on the false assumption that Rector’s invention can utilize only one of server-side or client-side verification. But as I explained in my first declaration, “[t]he server-side verification could also be done as a check on local verification.” Ex. 1005, ¶ 122. Utilizing both server-side and client-side verification, for example, in a multi-factor authentication scheme, would minimize or eliminate any security disadvantages associated with server-side verification alone. Just as having two locks on your door is more secure than one, a two-step, local and server-based authentication scheme would prevent a bad actor from obtaining access to the system should any one authentication method be compromised.

VII. CONCLUSION

22. I declare that all statements made herein of my knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: May 9, 2025

By: Kevin C Almeroth
Kevin C. Almeroth, Ph.D.