

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

TOYOTA MOTOR CORP,  
Petitioner,  
v.

AUTOCONNECT HOLDINGS LLC,  
Patent Owner.

---

PGR2025-00041  
Patent 12,039,243

---

**DECLARATION OF PAUL D. MARTIN, PH. D.**

## **TABLE OF CONTENTS**

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| I. INTRODUCTION .....                                                                | 7  |
| II. QUALIFICATIONS.....                                                              | 7  |
| III. MATERIALS CONSIDERED.....                                                       | 18 |
| IV. LEGAL STANDARDS.....                                                             | 19 |
| A. Patent Eligibility .....                                                          | 19 |
| B. Obviousness.....                                                                  | 20 |
| C. Claim Construction.....                                                           | 21 |
| V. LEVEL OF ORDINARY SKILL IN THE ART. ....                                          | 22 |
| VI. THE '243 PATENT .....                                                            | 23 |
| VII. SUMMARY OF THE ASSERTED REFERENCES.....                                         | 31 |
| A. Hendry .....                                                                      | 31 |
| B. Singh.....                                                                        | 36 |
| C. Poulsen.....                                                                      | 40 |
| D. Rovik.....                                                                        | 42 |
| E. Cazanias .....                                                                    | 45 |
| F. Forstall .....                                                                    | 45 |
| VIII. ANALYSIS OF PETITIONER'S GROUNDS OF UNPATENTABILITY ..                         | 46 |
| A. Ground 1: Claims 1-20 Are Patent Eligible Under Section 101. ....                 | 46 |
| 1. Technical Context for the Vehicle Profile Control Systems of the '243 Patent..... | 47 |
| 2. Overview of the Challenged Claims and Their Technical Requirements.....           | 51 |
| 3. Specification-Based Description of the Claimed Vehicle-Side Architecture .....    | 55 |
| 4. Technical Analysis of the Claims Under Alice Step One.....                        | 59 |
| 5. Technical Response to Petitioner's Characterization at Alice Step One.....        | 63 |
| 6. Technical Analysis of the Claims Under Alice Step Two .....                       | 66 |
| 7. Technical Response to Assertions of Conventionality .....                         | 69 |

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| 8. Summary of Technical Opinions Regarding Patent Eligibility.....                                                 | 71  |
| B. Ground 2: Claims 1, 6-8, 11, and 16-18 Would Not Have Been Obvious<br>In View of Hendry. ....                   | 73  |
| 1. Claims 1 and 11 .....                                                                                           | 73  |
| 2. Claims 6 and 16.....                                                                                            | 83  |
| 3. Claims 7-8 and 17-18 .....                                                                                      | 84  |
| C. Ground 3: Claims 2-7 and 12-17 Would Not Have Been Obvious over<br>Hendry in View of Poulsen.....               | 86  |
| 1. Claims 2 and 12 .....                                                                                           | 90  |
| 2. Claims 3 and 13 .....                                                                                           | 91  |
| 3. Claims 4 and 14.....                                                                                            | 93  |
| 4. Claims 5 and 15 .....                                                                                           | 94  |
| 5. Claims 6 and 16 .....                                                                                           | 95  |
| 6. Claims 7 and 17 .....                                                                                           | 95  |
| D. Ground 4: Claims 9-10 and 19-20 Would Not Have Been Obvious over<br>Hendry in view of Rovik. ....               | 96  |
| 1. Claims 9 and 19 .....                                                                                           | 96  |
| 2. Claims 10 and 20 .....                                                                                          | 103 |
| E. Ground 5: Claims 1, 6-7, 11, and 16-17 Would Not Have Been Obvious<br>over Singh.....                           | 106 |
| 1. Claims 1 and 11 .....                                                                                           | 106 |
| 2. Claims 6 and 16 .....                                                                                           | 112 |
| 3. Claims 7 and 17 .....                                                                                           | 112 |
| F. Ground 6: Claims 2-8 and 12-18 Would Not Have Been Obvious over<br>Singh in view of Cazanias and Forstall. .... | 112 |
| 1. Claims 2 and 12 .....                                                                                           | 118 |
| 2. Claims 3 and 13 .....                                                                                           | 118 |
| 3. Claims 4 and 14.....                                                                                            | 119 |
| 4. Claims 5 and 15 .....                                                                                           | 119 |
| 5. Claims 6 and 16.....                                                                                            | 120 |

|                                                                                                 |     |
|-------------------------------------------------------------------------------------------------|-----|
| 6. Claims 7-8 and 17-18 .....                                                                   | 120 |
| G. Ground 7: Claims 9-10 and 19-20 Would Have Been Obvious over Singh<br>in view of Rovik. .... | 121 |
| 1. Claims 9 and 19 .....                                                                        | 121 |
| 2. Claims 10 and 20 .....                                                                       | 122 |
| IX. CONCLUSION .....                                                                            | 122 |

## PATENT OWNER'S EXHIBIT LIST

| Exhibit | Description                                                                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2001    | <i>DigitalDoors, Inc. v. International Business Machines Corporation</i> , Case No. 2:22-CV-00457-JRG-RSP, ECF No. 41 (E.D. Tex. Jul. 24, 2023) (Gilstrap, J.)                  |
| 2002    | <i>Uniloc USA, Inc. v. Motorola Mobility LLC</i> , Case No. 2:16-CV-00992-JRG, ECF No. 125 (E.D. Tex. Apr. 5, 2017)) (Gilstrap, J.)                                             |
| 2003    | <i>Garrity Power Services LLC v. Samsung Electronics Co. Ltd. et al.</i> , Case No. 2-20-CV-00269-JRG, ECF No. 40 (E.D.Tex. Feb. 17, 2021) (Gilstrap, J.)                       |
| 2004    | <i>Clear Imaging Research, LLC, v. Samsung Electronics Co., Ltd.</i> , Case No. 2:19-CV-00326-JRG, ECF No. 127 (E.D.Tex. Dec. 21, 2020) (Gilstrap, J.)                          |
| 2005    | <i>Solas OLED Ltd. v. Samsung Display Co.</i> , No. 2:19-CV-00152-JRG, ECF No. 133, (E.D. Tex. July 17, 2020) (Gilstrap, J.)                                                    |
| 2006    | <i>Oyster Optics, LLV, v. Inferna Corp., et. al.</i> , Case No. 2:19-CV-00257-JRG, ECF No. 87 (E.D.Tex. July 17. 2020) (Gilstrap, J.)                                           |
| 2007    | First Amended Docket Control Order, <i>AutoConnect Holdings, LLC v. Toyota Motor Corp.</i> , No. 2:24-CV-00802-JRG-RSP, ECF No. 53 (E.D. Tex. February 13, 2025) (Gilstrap, J.) |
| 2008    | Lex Machina Median time to trial Statistics for EDTX for 5 years preceding EDTX proceeding                                                                                      |
| 2009    | Lex Machina Median time to trial Statistics for Judge Gilstrap for 5 years preceding EDTX proceeding                                                                            |
| 2010    | <i>Excerpts of Toyota's Invalidity Contentions served April 1, 2025, AutoConnect Holdings, LLC v. Toyota Motor Corp.</i> , No. 2:24-cv-00802-JRG-RSP (E.D. Tex.)                |
| 2011    | Guidance on USPTO's rescission of "Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation," March 24, 2025           |
| 2012    | USPTO FAQs for Interim Processes for PTAB Workload Management                                                                                                                   |
| 2013    | USPTO Office Action rejecting Toyota Patent App. No. 15/230,621 (US Patent No. 9,936,065) with Notice of References Cited, June 21, 2017                                        |
| 2014    | USPTO Office Action rejecting Toyota Patent App. No. 17/000,114 (US Patent No. 11,285,896) with Notice of References Cited, March 29, 2021                                      |

|      |                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------|
| 2015 | Information Disclosure Statement filed in Toyota Patent App. No. 17/829,583 (US Patent No. 12,079,616), June 1, 2022    |
| 2016 | Information Disclosure Statement filed in Toyota Patent App. No. 17/263,444 (US Patent No. 11,810,363), January 1, 2019 |
| 2017 | Declaration in Support of Todd S. Werner's Notice of Intent                                                             |
| 2018 | Declaration in Support of Motion for Pro Hac Vice Admission for William R. Woodford                                     |
| 2019 | Updated Declaration for William R. Woodford's Motion for Pro Hac Vice                                                   |
| 2020 | Email from Board authorizing stipulation to change due dates and changing oral argument date, November 19, 2025         |
| 2021 | <i>Curriculum Vitae</i> of Dr. Paul Martin                                                                              |
| 2022 | Declaration of Dr. Paul Martin                                                                                          |
| 2023 | Deposition Transcript of Mr. Scott Denning, January 5, 2026                                                             |

## **I. INTRODUCTION**

1. AutoConnect Holdings LLC (“AutoConnect” or “Patent Owner”) has requested my expertise in analyzing and providing opinions regarding this proceeding (PGR2025-00041) and the underlying ’243 patent at issue.

## **II. QUALIFICATIONS**

2. I am the Chief Scientist at Harbor Experts, Inc. and a part-time Lecturer in the Department of Computer Science at Johns Hopkins University. I hold B.S., M.S.E., and Ph.D. degrees from Johns Hopkins University, with all degrees, including my doctorate, being in computer science. My current curriculum vitae (CV) is attached to this declaration as Exhibit 2021.

3. I am an expert in the technical subject matter areas relevant to this case. All opinions and facts stated in this report are true and correct to the best of my knowledge. If called upon to testify, I could and would testify to the truth of the following. The company for which I work, Harbor Experts, is being compensated at the rate of \$675 per hour for time that I spend on this case. Harbor Experts is also being reimbursed for my reasonable and customary expenses. My compensation is not dependent in any way on the results of the lawsuit or the substance of my testimony.

4. I am a part-time lecturer in the Department of Computer Science at Johns Hopkins University. I currently teach classes on computer and network

security and applied cryptography, and C and C++ programming, developer tools and Linux environments. In the past I have taught classes on the topic of hardware hacking, including analyzing, modifying, and repairing computer hardware and embedded devices and vulnerability analysis and exploitation. I also occasionally substitute teach classes on network security and cryptography.

5. My classes cover a diverse array of topics including hardware and software security design, analysis and reverse engineering for vulnerability assessment; hardware and software-based attacks on computer components including RAM and CPUs; applied cryptography; computer architecture; computer networking; and component-level repair and modification. My classes also utilize hardware and software emulation and virtualization techniques to present students with a variety of real-world environments to learn and perform hands-on projects.

6. In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University. In fall 2011, I began working towards my Ph.D. in computer science, also at Johns Hopkins University, and I began researching computer security and privacy systems to both design novel technologies for securing computing systems and to also bridge the interface gap between users and their technology. As such, my research focused not only on developing technical solutions to novel security and privacy systems but to also presenting these solutions in a way that non-technical users could understand. Part of my research also focused on non-

deterministically generating virtualized computer networks in order to provide malware education environments for students. I also developed an emulator for analyzing malware code segments as part of a student project with the NSA. This emulator was integrated into an IDA Pro plugin and was able to observe how binary instruction snippets taken from malware samples modified their computing environment.

7. During my tenure as a Ph.D. student at Johns Hopkins, I was fully funded as a research assistant and/or teaching assistant throughout all my semesters. I was a member of the Upsilon Pi Epsilon computer science honor society, as well as its treasurer for the 2014-2015 school year. I was also a member of the Johns Hopkins chapter of the Association for Computing Machinery. I earned an award for outstanding teaching assistant in the Computer Science department for the year 2014-2015. I co-instructed a short course called, “Introduction to Hardware Hacking,” with a colleague, Dr. Michael Rushanan, which was the highest-rated course in the computer science department (based on student reviews) during the winter session in which it was offered. In this course, we offered lessons on a variety of topics including modifying game consoles and device firmware; electronics repair; binary analysis and modification, network traffic analysis; and web-based vulnerability assessment and exploitation.

8. During my time as a student at Johns Hopkins, I also participated in numerous kinds of service to the department. I represented the university as a student speaker at numerous open houses and admitted student days to help introduce prospective students to the computer science department. I was selected to speak to the external advisory board for the computer science department to provide insight into the student experience in the department. I served the department as the faculty liaison czar for several semesters, in which I attended and documented faculty meetings, which I then summarized for the students in the department. I also mentored and supervised a high school student on a year-long student project in software design and I supervised a variety of undergraduate research assistants on some of my research projects.

9. I finished my Ph.D. by successfully defending my dissertation, entitled “Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare,” on February 12, 2016, at the age of 26. My doctoral thesis tells the story of a secure healthcare practice of the future in which technology is seamless to use for healthcare providers while providing a much higher standard of security than is typical today. It focuses on the juxtaposition of usability and security with an emphasis on simplicity, automation, and error-proofing of security controls.

10. During my doctorate and afterward, I have produced, peer-reviewed, and published research in areas such as fingerprinting, anomaly detection,

multifactor authentication, and embedded systems security (which is applicable in many domains including the automotive domain). In many of these cases, I focused not only on designing novel security systems but also on designing usable web-based security systems for controlling them and understanding their data output. In fact, some of my research has formed the basis for commercial products and services. For example, in my work on integrated audit and access control, which was funded in part by Accenture Labs, I developed a Hadoop-based application to perform large-scale statistical analysis of audit logs from an electronic medical record system. As part of this work, I also designed a web application to automatically produce human-readable reports and graphs for use in consulting. Accenture subsequently patented this technology.

11. Similarly, in my research at Applied Communication Sciences in 2013, I designed and implemented a web-based traffic visualization dashboard and analysis system for field area smart grid networks that could be used to quickly gain an understanding of the current state of a SmartGrid network as well as to detect unexpected anomalies in the network. This dashboard was able to aggregate and visualize multiple data streams in realtime. Applied Communication Sciences subsequently patented this work and continued to build on the project. To my knowledge, they sold and/or still sell this product as part of their SecureSmart Managed Security Service product offering.

12. I have worked on and published two research projects related to improving the quality and ease-of-use of authentication technologies, especially in healthcare settings. In one project, my co-authors and I designed an indoor location tracking system consisting of unspoofable Bluetooth Low Energy beacons. These beacons were placed around a building and mapped to a backend such that a user could report which beacons he or she was within range of to be used as a secondary authentication mechanism for accessing patient medical records. In the way that we designed and envisioned the system, a doctor would log into a mobile device which would connect to a web-based backend. As the doctor walked past patient rooms, he or she would be automatically presented with medical records of nearby patients. In another project, my co-authors and I designed an authentication bracelet that would receive a Kerberos ticket upon login to a modified computer terminal through use of low-energy electrical signals transmitted over the wearer's skin. Upon use of other terminals throughout the hospital, this Kerberos ticket could be sent back over the wearer's skin to the custom contact on the terminal to allow the user to login without a password. The bracelet was also designed to immediately lose the cryptographic secret upon being removed from the user.

13. My recent research has focused primarily on embedded systems security with an emphasis on binary analysis, anomaly detection and automated security enforcement. In one case, I designed a security system that can be soldered

directly to the CPU of embedded devices to perform control-flow integrity for purposes of profile building and enforcement. In another case, I designed a system to automatically discern name and version information from binaries on embedded devices to build a software profile of the platform configuration of the device which can then be cross-referenced with a vulnerability database. I have also written a patent on this specific technique.

14. As of 2023 I am a member of the program committee for the IEEE Symposium on Security and Privacy. As a member of this committee, I peer review research that has been submitted for publication at the Symposium. I have recently reviewed research on memory forensics, side channel attacks, password vaults, differential privacy, computational theory, memory module design, and hardware security.

15. I am a named inventor on six patents. A full listing of these patents can be found on my CV, attached as Exhibit 2021.

16. In 2007, I developed my first Linux distribution and an associated LiveCD build system, called PJAMAS. The Linux distribution was built on Gentoo, a source-based Linux distribution, and compiled from scratch to be a minimal desktop image that could fully boot and run on low-performance desktop computers that primarily ran the Windows operating system, and that could run Windows binaries under the WINE libraries. The ultimate goal of the distribution was to

identify and remove malware from infected Windows computers. To achieve these goals, I tuned the kernel and operating system configuration, including performance-critical subsystems, to minimize RAM footprint, reduce runtime overhead, and constrain binary size, allowing the software to run on the widest possible range of Windows-era hardware. As an artifact of this process, I also produced a general-purpose build system for creating Gentoo-based Linux LiveCDs that could be custom-designed for any purpose.

17. This early work focusing on Linux, systems, and security became the focal point of my career and led me to select security, operating systems, and embedded systems as core areas of my professional work and research.

18. I began working in the software industry in 2008, when I obtained my first independent consulting client—Brandeis University. I created a program for their computer repair shop’s ticketing system to interface with a label printer. This enabled the computer repair shop to automatically print labels associated with tickets to easily identify customers’ devices.

19. Shortly after finishing my engagement with Brandeis University, I began working for the Johns Hopkins University Digital Research and Curation Center as a student programmer. There, I created a batch importer for a digital archiving system called DSpace to enable hundreds of digitally archived works per week to automatically be added to the repository. I next ported a web interface for

statistics tracking and visualization to the same digital archiving system to allow library staff to more easily visualize and understand data about how the digital archiving system was being used through a common web-based interface.

20. In 2009, I began working for a security consulting company called Independent Security Evaluators in Baltimore, Maryland. I worked on a wide variety of security and privacy projects including projects to test and break the DRM scheme of a magazine distribution application for IOS and Android (at the behest of the developer of said application), projects to test implementation code for cryptographic secret splitting, projects to assist with fuzz testing for security vulnerabilities of a variety of software applications, software development projects to automate testing of antivirus and antimalware solutions, and a variety of other security-related projects. Of note, I designed automation systems to create and restore virtualized snapshots of Windows machines on which I tested antivirus software on actual malware samples as part of a project for Consumer Reports. I worked for ISE as an intern throughout the semesters and summers until August 2011. In 2010, I also designed a security architecture for a large-scale digital curation system meant to be a major inter-university initiative to create a successor to existing digital curation systems that could be used for decades.

21. In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University, and I also retained an independent consulting client, the

University of Michigan, for whom I performed a penetration test and security assessment of a cloud-based research system that they planned to deploy.

22. In February 2016, I joined Harbor Labs full-time as a research scientist. In January 2019, I was promoted to Director of Firmware Analysis. In December 2023, I was promoted to Vice President of Applied Research and Technology. In October 2024, the division of Harbor Labs that I managed became Harbor Experts. I became Chief Scientist at Harbor Experts during this time. At Harbor Experts, I manage client engagements related to all the analysis work that Harbor Labs performs. I also lead Harbor Experts' research projects.

23. A significant portion of my role at Harbor Experts is in managing source code review engagements. As part of this work, I have reviewed software systems of varying sizes, often totaling millions or even billions of lines of code. I have reviewed products in the security space, television-based set top boxes, network appliances, numerous web-based enterprise systems, email management systems, telephony products, embedded system bootloaders, social network platforms, virtualization platforms and countless other products.

24. Prior to joining Harbor Experts, I was also the technical and development lead for a firmware security analysis engine for a product developed at Harbor Labs called Firmware IQ. Firmware IQ is designed to analyze the firmware of embedded devices for security vulnerabilities in an automated fashion. In one

configuration of the product, a developer uploads a firmware image to a web-based portal which uses a broker to forward the firmware to an engine for analysis. The engine unpacks the firmware, breaks it into its constituent components, and then performs more than a hundred automated security checks to find vulnerabilities in the firmware image. The results are then reported through JSON to a web-based presentation system which displays them in an interactive fashion.

25. Since Firmware IQ, I have devoted a substantial portion of my time to incorporating lessons learned from analyzing large numbers of firmware images into my own Linux distribution, which I am currently in the process of releasing. This distribution is intended to address several gaps in the current market.

26. I have also been involved in several automotive cases where I have provided litigation support performing infringement analysis and source code review. For example, I was engaged by OmniTracs in *OmniTracs, LLC v. Motive Technologies, Inc.*, which was related to driver fleet management, engaged by Uber in *AGIS Software Development LLC v. Uber Technologies*, which involved map overlays and messaging systems, engaged by BMW in *Onestra v. BMW*, as well as several other confidential engagements.

27. A more detailed list of my engagements can be found on my attached vita. Ex. 2021.

### III. MATERIALS CONSIDERED

28. In forming my opinions herein, I have considered the following documents:

| Materials Considered                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U.S. Patent No. 12,039,243 (Ex. 1001)                                                                                                                                                                                                                              |
| File History of U.S. Patent No. 12,039,243 (Ex. 1002)                                                                                                                                                                                                              |
| Declaration of Scott Denning (Ex. 1003)                                                                                                                                                                                                                            |
| <i>Curriculum Vitae</i> of Scott Denning (Ex. 1004)                                                                                                                                                                                                                |
| U.S. Patent App. Pub. No. 2012/0303178 to Hendry <i>et al.</i> (Ex. 1005)                                                                                                                                                                                          |
| U.S. Patent App. Pub. No. 2007/0276795 to Poulsen (Ex. 1006)                                                                                                                                                                                                       |
| U.S. Patent No. 8,918,231 to Rovik (Ex. 1007)                                                                                                                                                                                                                      |
| U.S. Patent App. Pub. No. 2007/0255464 to Singh <i>et al.</i> (Ex. 1008)                                                                                                                                                                                           |
| U.S. Patent No. 8,977,408 to Cazanias <i>et al.</i> (Ex. 1009)                                                                                                                                                                                                     |
| U.S. Patent App. Pub. No. 2009/0005070 to Forstall <i>et al.</i> (Ex. 1010)                                                                                                                                                                                        |
| U.S. Patent App. Pub. No. 2012/0254960 to Lortz <i>et al.</i> (Ex. 1011)                                                                                                                                                                                           |
| Microsoft Computer Dictionary, 5th Ed. (2002) (excerpted) (Ex. 1012)                                                                                                                                                                                               |
| U.S. Patent App. Pub. No. 2009/0325491 to Bell <i>et al.</i> (Ex. 1013)                                                                                                                                                                                            |
| Bluetooth Specification v2.1 (2007) (excerpted) (Ex. 1014)                                                                                                                                                                                                         |
| U.S. Patent No. 9,229,905 to Penilla <i>et al.</i> (Ex. 1015)                                                                                                                                                                                                      |
| U.S. Patent App. Pub. No. 2008/0205655 to Wilkins <i>et al.</i> (Ex. 1016)                                                                                                                                                                                         |
| U.S. Patent No. 8,863,256 to Addepalli <i>et al.</i> (Ex. 1017)                                                                                                                                                                                                    |
| U.S. Patent App. Pub. No. 2011/0078570 to Larsen <i>et al.</i> (Ex. 1018)                                                                                                                                                                                          |
| U.S. Patent App. Pub. No. 2010/0191748 to Martin <i>et al.</i> (Ex. 1019)                                                                                                                                                                                          |
| U.S. Patent App. Pub. No. 2014/0282931 to Protopapas (Ex. 1020)                                                                                                                                                                                                    |
| U.S. Patent App. Pub. No. 2013/0030645 to Divine <i>et al.</i> (Ex. 1021)                                                                                                                                                                                          |
| U.S. Patent App. Pub. No. 2004/0148526 to Sands <i>et al.</i> (Ex. 1022)                                                                                                                                                                                           |
| Barth, Matthew, <i>et al.</i> , “Interoperability Options for Shared-Used Vehicle Systems,” Transportation Research Record: Journal of the Transportation Research Board, No. 1887, TRB, National Research Council, Washington, D.C., 2004, pp. 137-144 (Ex. 1023) |

|                                                                                  |
|----------------------------------------------------------------------------------|
| U.S. Patent App. Pub. No. 2011/0195699 to Tadayon et al. (Ex. 1024)              |
| Toyota Motor Corp. v. AutoConnect Holdings LLC, PGR2025-00041, Papers 1, 6-7, 10 |
| Deposition Transcript of Mr. Scott Denning, January 5, 2026 (Ex. 2023)           |

29. Additionally, I have considered any exhibits that I have relied upon herein.

#### **IV. LEGAL STANDARDS**

##### **A. Patent Eligibility**

30. I understand that patent eligibility under 35 U.S.C. § 101 is evaluated using a two-step framework articulated by the Supreme Court and Federal Circuit, commonly referred to as the “Alice” framework. At step one, the inquiry asks whether the claim, considered as a whole in light of the specification, is directed to a law of nature, natural phenomena, or abstract idea. In making that determination, the focus is on the claimed invention, including the technical problem the claims and specification describe and the manner in which the claims purport to solve it, rather than on isolated claim elements viewed in the abstract.

31. If the claim is determined to be directed to excluded subject matter, the analysis proceeds to step two, which considers whether the claim includes an “inventive concept”—that is, whether the elements of the claim, individually or as an ordered combination, reflect more than what was well-understood, routine, and conventional in the relevant technical field at the time of the invention. I understand

that this inquiry may involve underlying factual considerations concerning the state of the art and how a person of ordinary skill would have understood and implemented the claimed system.

32. In forming my opinions, I apply this Section 101 framework from the perspective of a person of ordinary skill in the relevant field at the time of the invention, based on my technical experience, review of the '243 patent, and understanding of vehicle computing systems and their conventional design practices during the relevant period.

## **B. Obviousness**

33. I understand that a claim is unpatentable for obviousness if the differences between the claims and the applied references would have been obvious to a person of ordinary skill in art before the effective filing date of the claimed invention.

34. I understand that this process involves understanding the scope and content of the applied references, the differences between the claims and the applied references, and the level of ordinary skill in the art. I also understand that in some cases, the obviousness inquiry involves “secondary considerations” such as, for example, commercial success, long felt but unsolved needs, the failure of others, copying by competitors, industry praise, or unexpected results.

35. I also understand that to prove obviousness, a party must do more than just show that the claimed elements are known in separate references. Specifically, I understand that Petitioner must show that references teach or suggest the claimed elements, there would be a motivation to combine the teachings of the references to arrive at the claimed invention, and that a person of ordinary skill in the art would have had a reasonable expectation of success in performing the combination.

36. Additionally, I understand that obviousness cannot be sustained by mere conclusory statements. I have been informed that obviousness must be supported by articulated reasoning with some rational underpinning. Without an explanation as to the how or why references would be combined, an obviousness analysis is susceptible to hindsight reconstruction. I have been informed that hindsight reconstruction is a process in which the Patent Owner's claims are used as a roadmap for combining teachings in different references. I have also been informed that obviousness cannot be proven using hindsight reconstruction.

### **C. Claim Construction**

37. I have been informed that the Board construes claim using the same "Phillips" standard as district court. I understand that, as a general rule, claim terms are given their ordinary and customary meaning, namely the meaning that the term would have had to a person of ordinary skill in the art at the time of the invention. In construing patent claims, courts consider publicly-available sources that shed

light on how a person of ordinary skill in the art would have understood the claim language. Those sources include the claim language itself, the remainder of the specification, the prosecution history, and, when appropriate, extrinsic evidence such as technical literature, expert testimony, and information regarding the state of the art. I further understand there are two recognized exceptions to the general rule that claim terms are given their ordinary and customary meaning. The first is where the patentee has clearly set forth a special definition for the term, thereby acting as their own lexicographer. The second is where the patentee has clearly and unmistakably disavowed the full scope of a claim term, either in the specification or during prosecution.

#### **V. LEVEL OF ORDINARY SKILL IN THE ART.**

38. I understand that the earliest possible priority date for the '243 patent is April 15, 2013. I also understand that this date is not in dispute for this proceeding and use this date for the perspective of a person of ordinary skill in the art.

39. I understand that Petitioner has stated that a person of ordinary skill in the art, which Petitioner refers to as a POSA, “would have had at least a bachelor’s degree in computer science, electrical engineering, or a related field, and two years’ experience in data management or client-server systems and communications.” Petition at 6. I understand that Petitioner also states that “a higher education or skill level might make up for less experience, and vice-versa.” *Id.* I understand that Mr.

Denning has made similar statements. Ex. 1003 ¶ 37. For purposes of this declaration, I have applied this level of ordinary skill in the art.

40. In view of my education and experience as outlined above, I believe I am qualified to offer opinions from the perspective of a POSA as of the priority date of the '243 patent.

## **VI. THE '243 PATENT**

41. The '243 patent discloses a vehicle-based computing architecture that provides for secure access and management of individualized user profiles that govern how the vehicle operates, including vehicle functions and settings. Ex. 1001 at Abstract, 3:55-2:8; 43:64-44:31; 46:55-61; 58:35-47; 59:49-65:18; 62:52-62; 71:40-72:49; Fig. 23. Rather than treating profiles as generic data records, the disclosed systems integrate profile management into the vehicle's control architecture so that access to, and modification of, vehicle settings occurs under vehicle-side control. *Id.* at 43:64-44:29. The disclosed systems improve the reliability and security of such user profile management through explicit authentication and/or verification gating steps directly applied in response to requests to access and modify a vehicle-stored profile, using vehicle-resident hardware and processing. *Id.* at 71:40-58; 87:54-67. The patent describes optional coordination of profiles stored at mobile devices, servers, and other vehicles,

including conflict determination and reconciliation logic designed to preserve consistent vehicle behavior across distributed environments. *Id.* at 88:1-21.

42. The patent explains that user profiles are stored at the vehicle and include preferences associated with vehicle functions such as configuration settings, operational behaviors, and user-specific controls. *Id.* at 44:23–27; 57:65–58:20; 58:35–47; 59:49–64, Figs. 12A-12D. These vehicle-stored preferences are used by the vehicle system to personalize vehicle behavior across different vehicle sessions, ensuring that user-specific settings are consistently applied when the same user later accesses the vehicle. *Id.* at 23:26-33; 64:30-50; 71:59-63; 74:1-11; 74:47-55; 75:6-9; 88:1–4. The profile can include settings for vehicle components such as seat position, mirror position, infotainment system, navigation system, HVAC, and other vehicle subsystems. *Id.* at 62:48-62; 76:35–77:14.

43. In response to receiving a request to access a user profile, the vehicle system performs a verification process and/or an authentication process to determine whether the request is authorized. *Id.* at 71:40-58; 87:54-65; Fig. 23 (steps S2304, S2316-S2328). These authorization checks are performed by the vehicle system itself before any access to, or modification of, the vehicle-stored profile is permitted. By applying verification and/or authentication checks in response to profile access and modification requests, the system prevents unauthorized and inadvertent modification of vehicle-stored profiles and improves the security and reliability of

profile management within the vehicle. The verification and/or authentication processes involve vehicle-executed processing and can include biometric recognition, device identification, or other authentication techniques. *Id.* at 71:40-58; 72:52-59; 73:24-47; 87:54-68, claims 7-8, Figure 23 (S2320).

44. The '243 patent describes that the authentication processes:

can be based on the exchange of the security keys between the user, the vehicle, and/or even a server(s). This type of encryption may be cryptographically asymmetric in nature, such as private and public keys. In one example, a user may maintain a private key on a mobile device, and a public key may be provided by a vehicle, such a rental vehicle. In another example, the user may maintain the private key on the mobile device, and the private key may be provided by the vehicle, such as a rental vehicle. Other embodiments may use a private key on the communication device and a private key provided by the vehicle and/or a public key on the phone and a public key provided by the vehicle. In yet another embodiment, the exchange of keys may be facilitated via a certified trusted authority, similar to certificate of authority (CA).

*Id.* at 73:24-39; *see also id.* at 87:60-63, claim 8, Figure 23 (S2324).

45. Once the request is verified and/or authorized, the vehicle system determines one or more requested modifications to preferences associated with vehicle functions or settings. *Id.* at 87:63-65, Fig. 23 (S2328). The patent describes this sequencing as part of the vehicle's control flow, in which authorization precedes

any modification of vehicle settings. *Id.* at Fig. 23. These requested modifications are evaluated and handled by the vehicle's processors rather than being applied transiently or processed externally. *Id.* at 41:60-61; 43:64-44:12; 71:59-72:3, 92:66-93:21; Fig. 8A (848).

46. In response to the requested modifications, the vehicle system creates an updated user profile at the vehicle that includes one or more updated preferences based on the requested modifications. *Id.* at 73:56-61; 74:17-20; 87:65-67; Fig. 23. The updated profile is stored at the vehicle and governs how the vehicle will operate in subsequent vehicle sessions. *Id.* at 44:23-27; 57:65-58:20; 58:35-47; 59:49-64; 85:4-29, 85:43-86:9; Figs. 12A-12D.

47. This persistent storage of updated profiles ensures that authorized changes to vehicle functions and settings are consistently reapplied across different vehicle sessions, addressing technical problems associated with inconsistent vehicle behavior among multiple users or sessions. *Id.* at 23:26-33; 64:30-50; 71:59-63; 74:1-11; 74:47-55; 75:6-9; 88:1-4. The disclosure further teaches that profile updating is integrated into the vehicle's computing system to ensure consistency and security of vehicle-specific preferences. *Id.*; *see also id.* at 73:2-23.

48. By embedding authorization checks directly into the profile-access and modification process, the '243 patent addresses technical problems specific to vehicle-based systems, including unauthorized modifications, profile integrity, and

inconsistent vehicle behavior across uses. *Id.* at 23:26-33; 64:30-50; 71:59-63; 74:1-11; 74:47-55; 75:6-9; 88:1-4. The patent situates these controls in the context of vehicle operation, where configuration changes affect how the vehicle behaves during use. *Id.* at 44:23-27; 57:65-58:20; 58:35-47; 59:49-64; 85:4-29; 85:43-86:9; Figs. 12A-12D.

49. The '243 patent further discloses that, after an updated user profile is created and stored at the vehicle, the vehicle system can transmit the updated profile to one or more remote destinations, including a mobile device, a cloud server, a remote server, or another vehicle. *Id.* at 23:26-33; 64:30-50; 71:59-63; 72:39-49; 74:1-11; 74:47-55; 75:6-9; 88:1-4. Prior to such transmission, corresponding local user profiles may already be stored at those remote destinations. *Id.* at 88:1-21. In connection with profile transmission, the disclosed systems perform conflict identification processing to determine whether any conflicts exist between updated preferences in the vehicle-stored profile and preferences in the remotely stored profile. *Id.* Where conflicts are detected, the vehicle system can overwrite preferences or perform a reconciliation process that allows selective determination of which preferences should control. *Id.* at 88:4-21. These conflict identification and resolution steps ensure consistency and integrity of user profiles across multiple storage locations while preserving user control over profile updates, offering a

mechanism for improving the reliability of distributed profile management in multi-vehicle and multi-device environments. *Id.* at 88:12-21.

50. The patent also explains that user profiles can be based on one or more templates defining a structured organization of user preferences. *Id.* at 72:35-49, 72:60-73:23. In some embodiments, a user profile is created based on a global standard template that provides a common baseline of preferences and settings that can be shared across vehicles or vehicle manufacturers. *Id.* at 72:60-73:23. Users may personalize the template by modifying preferences, with those modifications being stored as part of the user profile and propagated through the profile synchronization processes. *Id.* at 72:35-49.

51. Thus, the '243 patent teaches a vehicle-resident system that receives profile access requests, authorizes those requests through verification or authentication, determines requested preference modifications, and creates and stores an updated user profile at the vehicle reflecting those modifications. *Id.* at 87:44-67. The vehicle-resident profile management may further be coupled with coordinated storage, synchronization, and conflict resolution across remote systems to improve consistency and reliability of user-specific vehicle behavior across different vehicles and usage contexts. *Id.* at 88:1-89:37.

52. Independent claim 1 sets forth:

1. A system, comprising:

memory;  
machine-readable instructions; and  
one or more processors to execute the machine-readable instructions to:  
receive a request to access a user profile stored at a vehicle, the user profile including one or more preferences associated with functions or settings of the vehicle;  
determine, by performing at least one of a verification process or an authentication process in response to the request, whether the request is authorized to access the user profile;  
in response to determining that the request is authorized to access the user profile, determine one or more requested modifications to at least one of the one or more preferences; and  
in response to the one or more requested modifications, create an updated user profile at the vehicle, the updated user profile including one or more updated preferences based on the one or more requested modifications.

Ex. 1001, claim 1.

53. Independent claim 11 sets forth:

11. A method, comprising:

receiving a request to access a user profile stored at a vehicle, the user profile including one or more preferences associated with functions or settings of the vehicle;

determining, by performing at least one of a verification process or an authentication process via one or more processors in response to the request, whether the request is authorized to access the user profile;

in response to determining that the request is authorized to access the user profile, determining, via the one or more processors, one or more requested modifications to at least one of the one or more preferences; and  
in response to the one or more requested modifications, creating, via the one or more processors, an updated user profile at the vehicle, the updated user profile including one or more updated preferences based on the one or more requested modifications.

Ex. 1001, claim 11.

54. The independent claims of the '243 Patent set forth a causal chain of instructions (claim 1) or steps (claim 11) that none of the asserted references teach or suggest individually, or in combination. Each of the elements 1[c-2] through 1[c-4] of claim 1 (as identified by Petitioner) reference the preceding element. For example, element 1[c-4] recites “in response to the one or more requested modifications ...” which references the determination of one or more requested modifications from element 1[c-3]. Likewise, element 1[c-3] recites “in response to determining that the request is authorized to access the user profile ...” which references the determination as to whether the request is authorized to access the user profile from element 1[c-2]. And, element 1[c-2] recites “... performing at least one of a verification process or an authentication process in response to the request ...” which references the received request to access the user profile stored at the vehicle from element 1[c-1]. The same is true for the elements of claim 11.

55. The independent claims set forth a cohesive set of instructions or method steps tying request authorization to user profile modifications and updates, not merely separate profile access and modification processes.

## **VII. SUMMARY OF THE ASSERTED REFERENCES**

56. The Petition sets forth several references, with Hendry and Singh being “primary” references, asserted alone in grounds 2 and 5, respectively, and four references—Poulsen, Rovik, Cazanias, and Forstall—being “secondary” references asserted in combination with the “primary” references in grounds 3-4, and 6-7.

### **A. Hendry**

57. Hendry (Ex. 1005) describes a system “for reinstating settings of at least one vehicle component” that operates in response to a request to establish a communications link received from an external device. Ex. 1005 Abstract, ¶¶ 1, 4. In Hendry’s system, the external device “transmits a request to the communications module 104 that identifies the external device 100 to the communications module 104. The communications module 104 uses the request from the external device 102 to determine that a user associated with the external device 100 is in the vehicle 10. Based on this determination, the communications module 104 notifies various vehicle component modules, which adjust user settings of the components, that the user is in the vehicle 10. For instance, the communications module 104 can notify

an HVAC module 108, a seat module 112, an A/V module 116, and a lighting module 120 that the identified user or external device 100 is in the vehicle 10.” *Id.* ¶ 13.

58. Hendry further explains that “the user settings system 102 uses a request from an external device 100 to establish the communications link to determine an identity of the user or the device” and authenticate an external device. *Id.* ¶¶ 19-20. Specifically, the communications module 104 compares a key transmitted by the external device during link-establishment to a stored key, and if “the keys match, the external device 100 is authenticated.” *Id.* ¶¶ 19, 27.

59. Hendry generally describes verification and authentication together, referring to the external device being “verified/authenticated” based on both “a key and a device identifier.” *Id.* ¶¶ 19, 27, 29, 33. However, Hendry does indicate “the term key refers to any suitable code, password, passcode, or string used to authenticate a device,” suggesting authentication is tied to key assignment/exchange. *Id.* ¶¶ 17, 19.

60. After successful verification/authentication of the external device, “the communications module 104 transmits a signal via a communication bus” to notify one or more vehicle component modules that the device “is in the vicinity of the vehicle 10.” *Id.* ¶ 20. After the external device is verified/authenticated and the one or more vehicle component modules are notified of the user/device proximity, the one or more vehicle component modules retrieves corresponding settings. *Id.* ¶ 21

(“Once the HVAC module 108 receives notification that an external device 100 and/or the user is in the vicinity of the vehicle 10, the HVAC module 108 will retrieve the HVAC settings associated with the user from the HVAC module datastore 110 and will adjust the HVAC system 40 in accordance with the settings.”), ¶ 22 (“When the seat module 112 receives notification that the external device 100 and/or the user is in the vicinity of the vehicle 10, the seat module 112 will retrieve the user’s personal seat settings from the seat module datastore 114.”), ¶ 23 (“When the A/V module 116 receives notification that the external device 100 or the user is in the vicinity of the vehicle 10, the AV module 116 will retrieve the user’s personal A/V settings from the A/V storage module 118.”), ¶ 24 (“When the lighting module 120 receives notification that the external device 100 or the user is in the vicinity of the vehicle 10, the lighting module 120 will retrieve the user’s personal lighting settings from the lighting module data store 122.”), ¶ 25 (“It is envisioned that other vehicle components can be controlled in the manner described above.”).

61. Hendry, therefore, uses authentication/verification of device based on a request to establish a general communications link to identify that a user/device is near the vehicle, and then follows the authentication and verification process by initiating a request for the personal settings of the user associated with the identified device. None of these disclosures, however, describe “receiv[ing] a request to access a user profile stored at a vehicle,” or “determin[ing], by performing at least one of a

verification process or an authentication process in response to the request, whether the request is authorized to access the user profile.” Rather these portions of Hendry describe (1) receiving a request to establish a communications link, (2) authenticating/verifying an external device based on the request to establish the communications link, and then (3) in response to determining a user/device is in the vehicle’s vicinity, retrieving/reinstating settings associated with the device.

62. Hendry’s process starts with a request to establish a communications link, not a request to access a user profile. Hendry explicitly states that this request “establishes communication with the external device 100” and the communications module 104. *Id.* ¶ 13 (“The exemplary user settings system 102 includes a communications module 104 which establishes communication with the external device 100. To establish a communications link with the communications module 104, the external device 100 transmits a request to the communications module 104 that identifies the external device 100 to the communications module 104.”). Hendry further states that “[o]nce a communications link is established, data is transferred via the communications link to the communications module 104 from the external device 100 and to the external device 100 from the communications module 104.”). *Id.* ¶ 15. Hendry analogizes this process to that of the Bluetooth® pairing protocol. *Id.* ¶ 17-18. In my opinion, a person of ordinary skill in the art would not associated Bluetooth® pairing with a request to access a user profile.

63. Hendry then states “the user settings system 102 uses a request from an external device 100 to establish the communications link to determine an identity of the user or the device. In essence, the user settings system 102 piggybacks the request to establish a communications link into a request to reinstate the personal settings of the user associated with the external device 100.” *Id.* ¶ 19. This is the only portion of Hendry that discusses a “request to reinstate the personal settings of the user.” In my opinion, a person of ordinary skill in the art would understand this to mean that the user settings system 102 initiates a request to reinstate the personal settings of the user after Hendry’s external device is authenticated, as explained in the six paragraphs following this statement. *Id.* ¶¶ 20-25.

64. Hendry also describes that “a user may opt to change or add his or her personal settings after some time,” and:

“[t]he user at any given time may opt to change the settings of one or more of the vehicle components, as shown at step 356. If the user does so, the user may be prompted by the user interface 122 to indicate if the adjusted settings of the one or more vehicle components are to be saved. If the user responds affirmatively, the adjusted settings are saved in a datastore associated with the vehicle component, as shown at step 358.”

*Id.* ¶ 31. Hendry never describes or suggests that changing settings is tied to authorization of a request to access a user profile.

## **B. Singh**

65. Singh (Ex. 1008) describes a “intelligent vehicle” that requires each driver to “scan their finger impression to gain access to the vehicle.” Ex. 1008 at Abstract. Singh describes that its system “allows multiple drivers to use the vehicle by authenticating them with their finger impressions which are saved by means of databases installed in the operating system.” *Id.* ¶ 3.

66. Singh describes its system is a result of “some major concerns about the security of the vehicle and the use of a single vehicle by different drivers. The preferences used by one driver are not suitable to the other driver” and, in its system, users’ “privacy and other preferences will also be maintained as their data will be isolated from other users.” *Id.* ¶ 2.

67. Singh describes that:

[t]he door of the vehicle is fitted with a password console and a finger impression scanning console locked by means of a metallic shutter. These are used to authenticate the driver of the driver so that the correct settings are applied for the driver. The password and the finger impression of the driver are saved on the database in the operating system on the hard drive of the vehicle. In order to gain access to the vehicle and drive it the driver has to first enter the password on the password keypad. As the driver enters the password on the keypad, it is checked by the controller in the vehicle database. If the password exists in the database, the controller will open the shutter of the finger impression scan console and will prompt the driver to provide the finger

impression. When the driver provides the finger impression, the controller will match the finger impression in the database. Upon finding a positive match, the controller will open the vehicle for the driver and will also load the vehicle settings and other services customized by that particular driver.

*Id.* ¶ 4.

68. Specifically, Singh describes that its password window “is used by the driver to start the vehicle opening process. The driver is required to punch his or her password on the password window console. This password activates controller which checks this password in the database by means of a software program. If matched, this step leads to opening of the finger impression scanning device for the driver to scan the finger impression.” *Id.* ¶ 22. Singh describes that the password window is a gatekeeping mechanism to limit access to the finger impression scanner. *Id.* ¶ 38 (“The driver is required to provide the password on the password window to get access to the finger impression scanning console.”).

69. Singh describes that “[t]he purpose of the finger impression scanner console is to record the finger impression scanned by the driver” which is used “to verify the identity of the driver.” *Id.* ¶¶ 23, 39. Singh describes this “second step” as follows:

When the driver scans the finger impression on the device, the Controller Unit captures the impression and provides a copy to the software program. The software program now finds the finger

impression in only the entries that contain the same password as entered by the driver. If it finds a match amongst those entries, it will return a positive result to the controller along with the name of the driver who scanned the finger impression. At this the Controller provides the notification on the results portion of the finger impression scanning console and closes it down in order to implement the next step.

*Id.* at 39. “The third step in the current invention is initiated only when the result from the second step is positive” where “the Controller Unit closes the Password Entry Console and unlocks the driver door of the vehicle. After the door is opened, the Controller Unit sends a signal to start the engine of the vehicle.” *Id.* ¶ 40; *see also* ¶ 23.

70. It is only after the vehicle door is opened and the vehicle is started that Singh begins its “Features Loading Program.” *Id.* ¶¶ 40-41 (“Once the verification has been performed and the vehicle started, the Controller Unit of the current invention loads the essential vehicle features for the driver. The Controller Unit initiates a Features Loading Program which installs all the essential features of the vehicle pertaining to the preferences of the driver and forwards a copy of the scanned finger impression to the Features Loading Program.”). Singh also describes an operator database that maintains user profiles containing “files with information and preferences of different drivers for features like Car Settings ...” *Id.* ¶ 33.

71. Accordingly, Singh describes a vehicle entry system requiring a password to open the fingerprint console, and a matching fingerprint to open the vehicle doors and start the vehicle. As illustrated in Figure 3, if no matching password is found, Singh’s process returns to password entry, and if no matching fingerprint is found, Singh’s process returns to fingerprint entry. *Id.* at Figure 3. Only after authenticating a user with the password and fingerprint (with Singh noting that different users may have the same password—*id.* ¶ 22), does Singh initiate a program to install the vehicle features for the driver stored in user profiles. Singh only initiates access to a user profile *after* the *user* is verified via his/her password and authenticated via his/her fingerprint. Singh fails to “*determine*, by performing at least one of a verification process or an authentication process *in response to the request*, whether the *request* is authorized to access the user profile.”

72. Singh also describes that its “invention enables each driver of the vehicle to make changes to their preference files by means of the Graphical User Interface. The driver can make changes to any or all the files as per the requirements. The driver will be able to make changes to the address file by amending the DriverName.AL file ... . The Controller Unit records all the modifications to the address file by means of the control program and prompts the user to save the changes just when the driver completes the task. *Id.* ¶ 62. Singh does not involve any security measures to limit the ability of vehicle occupants to make such changes.

73. Despite this disclosure, Singh never describes or even suggests that changing settings is tied to authorization of a request to access a user profile, like the independent claims set forth.

### **C. Poulsen**

74. Poulsen (Ex. 1006) describes “methods for creating, applying, using and retrieving profile information that includes attributes that may be stored separately from, or with, the content to which the profiles are being applied. In this manner, profiles can be shared in various environments and across various applications.” Ex. 1006 at Abstract.

75. Poulsen’s system is described with general applicability. For example, Poulsen explains that a user may wish to create a profile for “a document such as a Word document,” or “a set of CAD drawings” or even “an operating system user configuration.” *Id.* ¶¶ 35, 82. Poulsen’s reference to automobiles or vehicles are just one of many implementations.

76. Poulsen explains that a profile may include a plurality of attributes corresponding to configuration parameters, display settings, application states, or other environment-specific characteristics. *Id.* ¶¶ 2, 4-5. When a profile is applied, Poulsen describes iterating through the attributes of the profile—often via an attribute pointer—and applying each attribute to the selected content if the attribute is applicable and valid for that content. *Id.* ¶¶ 4, 51, 68, 78, Figs. 3, 9, 12. Poulsen

describes that users may choose to store some or all of a profile internally and/or externally. *Id.* ¶¶ 45-46. Poulsen continues that “[i]f the profile already exists within the documents or objects, the user may be prompted as to whether the existing profile should be updated, as well as to whether the profile should be completely overwritten or if only the attributes selected for storage should be updated (allowing the user to easily update a small number of settings without having to redefine the entire profile).” *Id.* ¶ 45; *see also id.* ¶¶ 47, 86-87.

77. Poulsen describes saving its profiles in manner similar to a “Save As” function, which prompts a user to confirm whether to overwrite an existing file with the same name, even if nothing within the document has changed. Poulsen never describes that its system compares the contents of an existing profile with the contents of the to-be-saved profile to determine if any conflicts exists. Indeed, Poulsen never uses the word “conflict” at all. Poulsen only states that a user may be prompted to decide what should or should not be overwritten. *Id.* ¶¶ 45, 47, 54, 57-58, 60-61, 63-64, 70-71, 83-84, 86-87 (“If the selected profile has previously been stored in the external location, the user may be prompted to confirm that the profile information should be changed or updated, as well as to determine whether the profile should be completely overwritten or if only the attributes selected for storage should be updated (allowing the user to easily update a small number of settings without having to redefine the entire profile.)” *see also id.* ¶¶ 89-90 (“if profile data

already exists in the selected storage location, the user may be prompted whether to overwrite the existing data.”).

**D. Rovik**

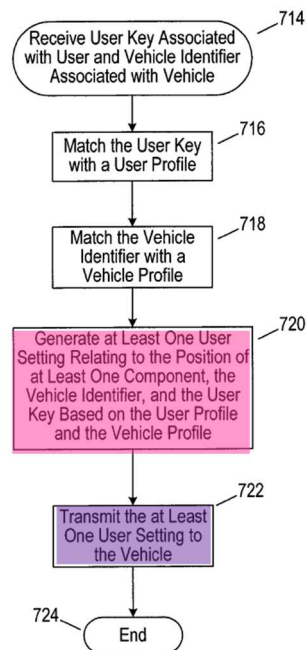
78. Rovik (Ex. 1007) describes “[a]pparatuses and methods for adjusting a position of at least one component of a vehicle.” Ex. 1007 at Abstract. Rovik acknowledges that adjustable components within vehicles are typically set for only that vehicle and users entering a “different make or model from the user’s usual vehicle ... will likely spend more time searching for their preferred settings.” *Id.* at 1:22-29. Rovik’s solution is to store “user settings at a server remote from a vehicle so that the user settings can be transmitted to different vehicles for the user.” *Id.* at 1:30-32.

79. Rovik does not use a common template across different vehicles. In contrast, Rovik explains that different vehicles from different manufacturers have different setting structures. Ex. 1007 at 8:7–10, 8:32–39, 8:55–59.

80. While Rovik describes a “standardized” user profile, Rovik describes it is used in combination with vehicle-specific profiles to generate new user settings for “vehicles having different geometries that the user has not driven before.” *Id.* at Figures 5-6, 9, 2:6-23; 8:66-10:25, 12:50-13:13. However, the “standardized” user profile is not a global standard template that is common among at least two vehicle manufacturers. Rather, these profiles represent “settings made by the user that have

been standardized by the server 400 so as to apply to a standard vehicle.” *Id.* at 9:37-40. The “standard vehicle” serves to provide a reference point to account for differences in the geometries between different vehicle models, e.g. a “distance of a track for a seat.” *Id.* at 13:2-6. In this way, the standardized profile is stored and used only at the remote server as a means for using settings saved for a “standard” vehicle to generate settings for a different vehicle model. After this process, the vehicle-specific settings (which differ based on model) are sent to the vehicle. Rovik never teaches that these standardized profiles are transmitted to different vehicles as suggested by Petitioner and Mr. Denning.

81. Rovik explains this process in more detail with reference to Figure 9, reproduced below.



82. Rovik explains that vehicle profiles 514 and 516 comprise “the geometries of the associated vehicles and the availability/capabilities of various vehicle systems” and ratios/deviations relative to attributes of a standard vehicle. *Id.* at 10:6-16. Rather than transmitting Rovik’s user profiles to different vehicles, Rovik instead **generates** “at Least One User Setting Relating to the Position of at Least One Component, the Vehicle Identifier, and the User Key Based on the User Profile and the Vehicle Profile.” *Id.* at Figure 9 (step 720), 13:2-6 (“generating a new user setting can involve using a user attribute in the user profile, such as a hip point, in combination with a vehicle attribute in the vehicle profile, such as a total distance of a track for a seat, to calculate a user setting for a position of a component, such as the seat 124.”); *see also* Figures 5-6, 9, 2:6-23; 8:66-10:25, 12:50-13:13.

83. In my opinion, a person of ordinary skill in the art would understand that Rovik is converting standardized user profiles into vehicle-specific user settings for transmission to new vehicles. Indeed, after generating the new user settings, Rovik describes **transmitting** these calculated new vehicle-specific user settings (not the “standardized” user profile) to the vehicle. *Id.* at Figure 9 (step 722), 13:10-13. In my opinion, a person of ordinary skill in the art would understand that these new vehicle-specific user settings sent to the vehicle would differ due to Rovik’s discussion about the variations of vehicle configures, geometries, and capabilities.

**E. Cazan**

84. Cazan (Ex. 1009) describes “technologies to allow transfer of a driver’s profile with one or more settings for user configurable features of a vehicle to and/or from a server via network communications.” Ex. 1009 at 1:44-48. Cazan describes that “settings input and stored for one vehicle may be uploaded to the server and later transferred to a different vehicle.” *Id.* at 1:48-51.

85. Cazan does not describe performing authentication or verification in response to a request to access a user profile stored at a vehicle.

**F. Forstall**

86. Forstall (Ex. 1010) describes methods and devices for “receiving, at a mobile device, location information stored in a memory of a vehicle device, and updating a mobile device based on the location information, where the mobile device is proximate to the location of the vehicle device,” and “transmitting to a vehicle device location information stored in a memory of a mobile device, and updating the vehicle device based on the location information, where the mobile device is proximate to the location of the vehicle device.” Ex. 1010 ¶¶ 6, 8.

87. Forstall also describes an “auto-update device or vehicle with new information” button, which when activated automatically provides new information to the other device. *Id.* ¶ 90. Forstall also describes a “resolve conflict in favor of” selector, which “determines which device’s information is copied onto the other

device” when “conflicts occur between information stored in the mobile device 100 and vehicle device(s) 405.” *Id.*

88. Forstall does not, however, discuss user profiles or user profile data. Rather, Forstall concerns mobile and vehicle location information from systems such as, for example, “global positioning system (GPS) or other positioning systems (e.g., systems using Wi-Fi access points, television signals, cellular grids, Uniform Resource Locators (URLs))” or “accelerometer 172, compass 173, and gyro 175.” *Id.* ¶¶ 36, 45, 57 61, 65, 68, 71-72, 75-77, 80, 84, 94.

## **VIII. ANALYSIS OF PETITIONER’S GROUNDS OF UNPATENTABILITY**

89. Petitioner sets forth seven separate grounds in its Petition. Each are addressed below.

### **A. Ground 1: Claims 1-20 Are Patent Eligible Under Section 101.**

90. I have been asked to provide my technical opinions regarding whether claims 1–20 of the ’243 patent are directed to an abstract idea and, if so, whether they recite an inventive concept. In forming these opinions, I have considered the claims as a whole and in light of the ’243 patent’s specification, from the perspective of a person of ordinary skill in the art at the time of the invention.

91. My analysis therefore addresses both steps of the framework used to evaluate patent eligibility. First, I address whether the challenged claims are directed to an abstract idea or instead to a concrete technological solution, taking into account

the technical problems identified in the specification and the manner in which the claimed systems and methods address those problems. Second, in the alternative and assuming for purposes of analysis that the claims were considered to involve an abstract idea, I address whether the claims recite an inventive concept, including whether the claimed combination and system architecture reflect more than what was well-understood, routine, and conventional in passenger vehicle computing systems at the time of the invention.

92. As explained below, my opinions are grounded in the technical context of modern vehicle computing systems, the specific requirements of the challenged claims, and the detailed disclosures of the '243 patent regarding vehicle-side control of profile access, modification, and synchronization.

### **1. Technical Context for the Vehicle Profile Control Systems of the '243 Patent.**

93. Modern vehicles are controlled by distributed computing systems that govern a wide range of vehicle functions and settings. These functions include not only convenience or infotainment features, but also settings that directly affect vehicle operation, driver positioning and visibility, access control, and passenger safety. As described in the '243 patent, vehicle computing systems use stored configuration data to control how vehicle subsystems operate during use. Ex. 1001 at Abstract, 3:55-2:8; 43:64-44:31; 46:55-61; 58:35-47; 59:49-65:18; 62:52-62; 71:40-72:49; Fig. 23

94. In this technical context, user profiles are not merely informational records. Rather, they store preferences associated with vehicle functions or settings that are applied by the vehicle's computing system to configure hardware components and software subsystems. When a profile is applied, the vehicle's control system uses the stored preferences to determine how the vehicle behaves during operation and across vehicle sessions.

95. The '243 patent explains that user profiles may include preferences relating to, for example, seating and mirror positions, infotainment behavior, navigation settings, HVAC operation, access restrictions, and other vehicle subsystems. *Id.* at 62:48-62; 76:35-77:14. These preferences are stored at the vehicle and are used by the vehicle computing system to personalize and control vehicle behavior for a particular user. *Id.* at 44:23-27; 57:65-58:20; 58:35-47; 59:49-64, Figs. 12A-12D.

96. Because user profiles are used to control vehicle operation, changes to a profile can immediately and materially affect how the vehicle behaves. From a technical perspective, this distinguishes vehicle user profiles from generic profile data used in ordinary consumer software systems. In a vehicle environment, profile data is functionally coupled to the control logic of a physical machine.

97. From a technical standpoint, because these preferences are applied by the vehicle computing system to control how a physical vehicle operates, errors,

inconsistencies, or unauthorized changes to profile data can have consequences that extend beyond user experience to system reliability and safe vehicle operation.

98. The specification recognizes that improper handling of vehicle profiles can lead to technical problems. For example, unauthorized or inadvertent modification of vehicle-stored profiles may result in inconsistent or unsafe vehicle behavior, particularly if configuration changes occur while a vehicle is in use. *Id.* at 59:17-48, 85:4-29, 85:43-86:9, 92:23-60, Figures 12A-12D. A person of ordinary skill in the art would understand that managing access to, and modification of, vehicle profiles in a controlled manner would preserve system integrity and reliability.

99. The '243 patent further explains that vehicle profile management often occurs in a distributed computing environment. *Id.* at 23:26-33, 64:30-50, 71:59-63, 72:39-49, 74:1-11, 74:47-55, 75:6-9, 88:1-4. User profiles may be stored not only at the vehicle, but also at mobile devices, servers, or other vehicles associated with the same user. *Id.* In such environments, profile updates made in one location can conflict with profiles stored elsewhere, creating the potential for inconsistent configuration state. *Id.* at 88:1-21.

100. In my opinion, these issues raise technical questions about where authoritative control over vehicle configuration should reside and how consistency should be maintained across systems. In this regard, the patent addresses how to

prevent unauthorized access, how to avoid conflicting profile updates across different storage locations, and how to ensure that vehicle behavior remains consistent and reliable over time. *Id.* at 87:44-88:21.

101. From an engineering perspective, these challenges do not dictate a single implementation. Instead, they require architectural choices about where control, authorization, and enforcement should reside within a distributed vehicle computing environment.

102. The patent describes these challenges in the context of vehicle-side control of profile access and modification. For example, it explains that access to and modification of a user profile may be conditioned on verification and/or authentication performed by the vehicle system, and that updated profiles may be stored at the vehicle and later transmitted to other systems in a controlled manner. *Id.* at 87:44-88:4; Fig. 23.

103. From the perspective of a person of ordinary skill in the art at the time of the invention, these disclosures reflect technical problems specific to computer-controlled vehicles, rather than generic data-processing concerns. In particular, such a person would understand the importance of enforcing authorization at the vehicle before allowing profile access or modification, sequencing authorization ahead of configuration changes, and managing how profile updates propagate across distributed systems to preserve consistent and safe vehicle operation.

104. Addressing these issues requires deliberate system-architecture choices. Vehicle profile management systems must determine where profile data is stored and enforced, how access is authorized and verified, when modifications are permitted, and how updated profiles are synchronized or reconciled across systems. These are technical design decisions that affect how the vehicle computing system operates and how it maintains control over vehicle behavior.

105. As discussed in the sections below, the '243 patent is directed to a vehicle-side profile control architecture designed to address these technical challenges by placing authorization, enforcement, and profile creation at the vehicle and by constraining how vehicle-created profile updates are propagated and reconciled across other devices and systems.

## **2. Overview of the Challenged Claims and Their Technical Requirements**

106. The claims of the '243 patent recite a vehicle-based computing system and corresponding method that govern how user profiles associated with vehicle functions or settings may be accessed, modified, and persisted. *See* Claims 1-20. From a technical perspective, the claims describe how a vehicle computing system controls configuration state that determines how the vehicle operates.

107. Each independent claim begins with a user profile that is stored at the vehicle. *See* Claims 1, 11. The claims expressly require that the user profile include “one or more preferences associated with functions or settings of the vehicle.” These

preferences are not described as abstract data, but as configuration parameters used by the vehicle computing system to control vehicle behavior.

108. The claims further require that, in response to a request to access the vehicle-stored user profile, the vehicle system determine whether the request is authorized. This determination is made by performing at least one of a verification process or an authentication process in response to the request.

109. Importantly, the claims require that this authorization determination occur before any modification of vehicle-related preferences is determined or applied. Only after the vehicle system determines that the request is authorized may it determine one or more requested modifications to the preferences associated with vehicle functions or settings.

110. Following authorization and determination of the requested modifications, the claims require that the vehicle system create an updated user profile at the vehicle. The updated profile includes one or more updated preferences based on the requested modifications and is stored at the vehicle to govern subsequent vehicle operation.

111. This sequence—request, authorization, determination of requested modifications, and creation of an updated vehicle-stored profile—is explicit in the claim language. From an engineering standpoint, it constrains when and how

configuration changes affecting vehicle behavior may occur and places control of those changes at the vehicle computing system.

112. The dependent claims further specify how this vehicle-side profile control is implemented. Certain dependent claims require that both verification and authentication be performed, and that authorization be determined only if both processes are successful. Claims 6, 16.

113. Other dependent claims specify technical mechanisms that may be used for verification or authentication, including biometric recognition, gesture or facial recognition, identification of a mobile device, and security key exchanges between the vehicle and a mobile device. Claims 7, 8, 17, and 18.

114. Additional dependent claims address what occurs after an updated user profile is created at the vehicle. These claims require transmitting the updated profile from the vehicle to one or more remote destinations, such as a mobile device, cloud server, remote server, or another vehicle, where a local user profile already exists. Claims 2 and 12.

115. The dependent claims further require determining whether conflicts exist between updated preferences in the vehicle-created profile and preferences stored in a local profile at the remote destination. Where conflicts are identified, the claims require either overwriting conflicting preferences or performing a

reconciliation process that allows selective determination of which preferences should control. Claims 3-5, 13-15.

116. From a technical perspective, these limitations constrain how vehicle-created configuration state propagates across distributed systems and how inconsistencies are resolved. The claims do not merely provide for data transmission; they require conflict identification and resolution logic to preserve consistent profile state.

117. Still other dependent claims require that user profiles be based on templates, including optional global standard templates common among multiple vehicle manufacturers. Claims 9, 10, 19, and 20. These limitations impose structure on how vehicle preferences are organized and shared, promoting consistency and interoperability across vehicles and systems.

118. When considered as a whole, the challenged claims require a vehicle computing system that stores user profiles at the vehicle, enforces authorization through vehicle-executed verification and/or authentication, requires authorization before determining or applying modifications to vehicle-related preferences, creates updated user profiles at the vehicle, and manages how those vehicle-created profiles are propagated and reconciled across other systems.

119. From the perspective of a person of ordinary skill in the art, these requirements define a specific system architecture and control flow tailored to

vehicle computing environments, rather than a generic process for managing information.

### **3. Specification-Based Description of the Claimed Vehicle-Side Architecture**

120. The '243 patent repeatedly emphasizes that access to and modification of user profiles governing vehicle behavior are not treated as ordinary data edits, but as controlled operations executed by the vehicle system itself. *Id.* at 71:40-58; 87:54-67. The specification explains that profile access and modification are conditioned on authorization logic implemented at the vehicle, and that such authorization is evaluated before changes are permitted. *Id.*

121. For example, the specification explains that when a request to access or modify a user profile is received, the vehicle system determines whether the request is authorized and only allows modification if that authorization is successful. *Id.* at 87:44-88:4, Figure 23.

122. This disclosure situates authorization as a gating operation performed by the vehicle system as part of its control logic, rather than as a peripheral or optional feature.

123. The specification further explains that verification and authentication may involve concrete technical mechanisms, including biometric recognition, device identification, and cryptographic exchanges. *Id.* at 71:40-58; 72:52-59; 73:24-47; 87:54-68, claims 7-8, Figure 23 (S2316-S2324). These mechanisms are

described as being executed by the vehicle computing system to determine whether a user or device is permitted to access and modify vehicle-stored profiles. *Id.* at 87:63-65; Figure 23 (S2328).

124. From a technical perspective, these disclosures reflect a deliberate system design in which security and access control are integrated into the vehicle's operational control path. The patent also makes clear that updated user profiles are created and stored at the vehicle and are used by the vehicle computing system to govern vehicle behavior going forward. *Id.* at Abstract, 3:55-2:8; 43:64-44:31; 46:55-61; 58:35-47; 59:49-65:18; 62:52-62; 71:40-72:49; Fig. 23.

125. The specification describes profile editing, saving, and storage as vehicle-resident operations that persist across vehicle sessions. *Id.* at 71:40-58, 87:44-88:21.

126. This disclosure reflects an architectural choice in which the vehicle maintains control over its configuration state, rather than relying on externally created profiles to dictate vehicle operation. From a technical standpoint, treating the vehicle as the authoritative source of configuration state addresses issues unique to vehicle systems.

127. Because vehicle settings directly affect physical operation, allowing external systems to create or impose configuration state without vehicle-side enforcement introduces risks related to reliability, latency, and safety. The

specification's repeated emphasis on vehicle-stored and vehicle-applied profiles reflects awareness of these concerns.

128. The specification also addresses the technical challenges that arise when user profiles exist in multiple locations, such as at vehicles, mobile devices, servers, or other vehicles. *Id.* at 88:1-21. The patent explains that transmitting updated profiles to other systems can result in conflicts when different versions of a profile exist. *Id.*

129. To address this problem, the '243 patent describes identifying conflicts between preferences in a vehicle-created profile and preferences stored at other locations and resolving those conflicts either by overwriting preferences or by performing a reconciliation process that allows selective determination of which preferences should control. *Id.* at 88:12-21. These disclosures show that the invention is concerned with maintaining consistent configuration across distributed systems while preserving vehicle-side control.

130. From a technical perspective, conflict identification and reconciliation of vehicle configuration profiles is not a generic data-synchronization problem. In a vehicle environment, inconsistent configuration state can lead to unpredictable or unsafe vehicle behavior. The specification's discussion of conflict handling reflects a system-level approach to preserving reliability and consistency of vehicle operation across devices and vehicles.

131. The '243 patent further explains that user profiles may be based on templates that define a structured organization of vehicle preferences. *Id.* at 72:35-49, 72:60-73:23. The specification describes the use of templates, including global standard templates common among multiple vehicle manufacturers, as a way to provide a consistent baseline for vehicle configuration while allowing user-specific customization. *Id.* at 72:60-73:23.

132. From a technical standpoint, template-based profile design imposes structure on how vehicle preferences are defined, stored, and shared. This structure facilitates interoperability and consistency across vehicles and systems and further distinguishes the claimed invention from unstructured or ad hoc profile editing.

133. The specification's discussion of templates reinforces that the claimed system is directed to structured control of vehicle configuration state, rather than to free-form manipulation of user data.

134. Taken together, these disclosures demonstrate that the '243 patent is directed to a vehicle-side control architecture in which authorization, enforcement, profile creation, and configuration persistence are integrated into the vehicle computing system itself. The specification consistently situates these operations within the vehicle's control logic and ties them to the problem of safely and reliably managing vehicle behavior.

135. From the perspective of a person of ordinary skill in the art, the specification does not describe generic profile management implemented on a vehicle. It describes a vehicle computing system designed to control when and how vehicle configuration state may be accessed, modified, stored, and synchronized, with attention to security, consistency, and operational reliability.

#### **4. Technical Analysis of the Claims Under Alice Step One**

136. In evaluating whether the challenged claims are directed to an abstract idea, I consider the claims as a whole and in light of the '243 patent's specification, including the patent's detailed description of vehicle-side authorization, profile creation, and control of configuration state, as discussed above, from the perspective of a person of ordinary skill in the art at the time of the invention. From a technical standpoint, this inquiry focuses on the character of the claimed system and what the claims require the system to do, rather than on isolated claim elements viewed in the abstract.

137. When read in this manner, the challenged claims are directed to a vehicle-side computing architecture that governs access to, and modification of, user profiles stored at the vehicle and associated with vehicle functions or settings. The claims define how authorization is performed, when configuration changes are permitted, and where authoritative profile state is created and stored.

138. As discussed above, the claims require that a user profile be stored at the vehicle and include preferences associated with vehicle functions or settings. Claims 1, 11. The specification explains that these preferences are applied by the vehicle computing system to control how the vehicle operates during use and across vehicle sessions. *Id.* at Abstract, 3:55-2:8; 43:64-44:31; 46:55-61; 58:35-47; 59:49-65:18; 62:52-62; 71:40-72:49; Fig. 23. From a technical perspective, the claims therefore concern control of vehicle configuration state, not merely the handling of informational data.

139. A central feature of the claimed system is that access to, and modification of, the vehicle-stored profile is conditioned on authorization performed by the vehicle system itself. Claims 1, 11. In response to a request to access the profile, the vehicle system must perform at least one of a verification process or an authentication process to determine whether the request is authorized. The specification describes this authorization as part of the vehicle's control logic for profile access and modification. *Id.* at 87:44-67, Figure 23.

140. The patent explains that authorization may involve technical security mechanisms such as biometric recognition, identification of a mobile device, or cryptographic exchanges between the vehicle and a device. *Id.* at 71:40-58; 87:54-65; Figure 23 (steps S2304, S2316-S2328). These mechanisms are performed by

the vehicle computing system and determine whether profile access and modification are permitted. *Id.*; *see also id.* at 43:64-44:29.

141. The claims further require that authorization be determined before requested modifications to vehicle-related preferences are determined or applied. Claims 1, 11. Only after the vehicle system determines that the request is authorized may it determine requested modifications and create an updated user profile at the vehicle. This authorization-first sequence constrains system behavior and governs when configuration changes affecting vehicle operation may occur.

142. The specification describes this sequence as part of the vehicle's profile editing and saving process, in which authorization gates access to profile modification and the updated profile is stored at the vehicle. *Id.* at 87:44-67, Figure 23. From an engineering standpoint, this ordered control flow reflects a system design in which the vehicle maintains control over changes to its configuration state.

143. The dependent claims further reinforce this vehicle-side control architecture by specifying how authorization and profile management are implemented. For example, certain claims require both verification and authentication, specify concrete authentication mechanisms, or require conflict identification and reconciliation when vehicle-created profiles are transmitted to other systems where profiles already exist. Claims 6, 7, 8, 16, 17, 18, 2-5, and 12-15.

144. In a distributed environment, the claims require that conflicts between preferences in a vehicle-created profile and preferences stored elsewhere be identified and resolved through overwriting or selective reconciliation. Claims 3–5 and 13–15. A person of ordinary skill in the art would understand that such conflict handling helps preserve consistency of profile state across systems while maintaining control over vehicle behavior.

145. Other dependent claims require that profiles be structured using templates, including optional global standard templates shared among vehicle manufacturers. Claims 9, 10, 19, and 20. From a technical perspective, these limitations further define how vehicle configuration data is organized and managed, and they reinforce that the claimed system concerns structured control of vehicle settings rather than unstructured data editing.

146. From the perspective of a person of ordinary skill in the art, the claims therefore describe a concrete vehicle computing solution that addresses technical issues arising from controlling access to and modification of vehicle configuration state. The claims define where control resides (at the vehicle), how access is authorized, when modifications are permitted, and how updated profiles are stored and coordinated across systems.

147. In my opinion, from the perspective of a person of ordinary skill in the art, the technical focus of the claims is on the operation, security, and reliability of

vehicle computing systems that control vehicle behavior. The claims are not directed to the abstract idea of “profile management” in isolation, but to a specific vehicle-side architecture for managing configuration state that governs how a vehicle operates.

## **5. Technical Response to Petitioner’s Characterization at Alice Step One**

148. I have reviewed the Petition and the Denning declaration with respect to their characterization of the challenged claims under Alice Step One. From a technical perspective, their analysis describes the claims at a level of abstraction that does not reflect how a person of ordinary skill in the art would understand the claimed system when read as a whole and in light of the specification.

149. In particular, the Petition characterizes the claims primarily in terms of generic actions such as “receiving,” “determining,” “updating,” and “transmitting” information. Pet. at 20–23; Ex. 1003 ¶¶ 132–135. While those words appear in the claim language, that characterization does not account for where those actions occur, under what conditions they occur, or how they affect the operation of the vehicle computing system.

150. The claims do not permit these actions to occur in an unconstrained or generic manner. Claims 1, 11. They require that a user profile be stored at the vehicle, that authorization be determined by the vehicle system through verification and/or authentication, that authorization occur before any modification is determined

or applied, and that the updated profile governing vehicle operation be created at the vehicle. From a technical standpoint, these constraints define a specific control architecture rather than an abstract information-processing concept.

151. The Petition’s characterization also does not account for the nature of the data being controlled. As discussed above, the preferences stored in the user profile are associated with vehicle functions or settings and are applied by the vehicle computing system to control how the vehicle operates. Treating such preferences as generic “information” divorced from system behavior does not reflect how they function in a vehicle computing environment.

152. The Denning declaration similarly treats the claims as involving routine data management or generic computer functions, without analyzing how the claims allocate control to the vehicle or require authorization-first sequencing before configuration changes affecting vehicle operation. 1003 ¶¶ 132–135, 140–145. From a technical perspective, the claims’ requirement that authorization and enforcement occur at the vehicle, prior to modification, is a defining architectural feature that is not captured by the Petition’s abstraction.

153. The Petition also suggests that the claimed steps could be performed mentally or with pen and paper. Pet. at 24–25. In my opinion, that suggestion does not account for the technical requirements of the claims. The claims require a vehicle computing system that performs verification and/or authentication, conditionally

permits access to vehicle-stored profiles, and creates updated profiles that govern vehicle behavior. These are system-enforced operations performed by vehicle computing hardware and software, not mental activities.

154. In addition, several dependent claims require technical mechanisms such as biometric recognition, mobile device identification, security key exchanges, conflict identification across distributed systems, and reconciliation of conflicting profile data. Claims 3–5, 7, 8, 13–15, 17, and 18. These operations involve technical processes that cannot be meaningfully performed by a human mind and further illustrate the system-level nature of the claimed invention.

155. From the perspective of a person of ordinary skill in the art, the Petition’s characterization omits the claim-imposed constraints that determine how the system operates and how vehicle configuration state is controlled. When those constraints are considered—as the specification repeatedly emphasizes—the claims describe a vehicle-side profile control system that governs access to and modification of vehicle settings under defined conditions.

156. For these reasons, I do not agree with the Petition’s characterization of the claims as being directed to abstract information processing. In my technical opinion, from the perspective of a person of ordinary skill in the art, the claims are directed to a concrete vehicle computing architecture that controls how vehicle configuration state is accessed, modified, and maintained.

## **6. Technical Analysis of the Claims Under Alice Step Two**

157. I have also considered whether the claims recite an inventive concept when evaluated as an ordered combination from the perspective of a person of ordinary skill in the art at the time of the invention.

158. From a technical standpoint, this inquiry does not turn on whether individual elements—such as verification, authentication, profile storage, or data transmission—were known in isolation. Rather, it turns on whether the claimed combination and system architecture, implemented in the context of vehicle computing systems, reflects activity that was well-understood, routine, and conventional at the relevant time.

159. The challenged claims define a coordinated vehicle-side control architecture in which authorization, enforcement, and profile creation are allocated to the vehicle computing system itself. The claims further require an authorization-first sequence before any modification of vehicle-related preferences is determined or applied, and they constrain how vehicle-created profiles are propagated and reconciled across distributed systems.

160. From an engineering perspective, this combination reflects a deliberate system design choice rather than a routine or inevitable implementation. In many distributed computing environments, profile or configuration data is modified externally—such as on a server or user device—and then transmitted to a client

system. The claims here require a different approach: the vehicle itself determines authorization, creates the updated profile, and serves as the authoritative source of configuration state governing vehicle operation.

161. The specification describes this vehicle-side allocation of control in the context of preventing unauthorized or inadvertent configuration changes and preserving consistent vehicle behavior. These disclosures reflect technical considerations specific to computer-controlled vehicles, where configuration changes directly affect vehicle operation and may have safety implications.

162. The claims also require a specific authorization-first control flow. Authorization must be determined by the vehicle system before requested modifications are determined and before an updated profile is created. From a technical standpoint, this sequencing constrains system behavior and alters how the vehicle computing system responds to access requests and configuration changes.

163. The dependent claims further reinforce the claimed architecture. Certain claims require both verification and authentication and specify technical mechanisms for performing those functions. Claims 6–8 and 16–18. Other claims require identifying conflicts between vehicle-created profiles and profiles stored at other locations, and then resolving those conflicts through overwriting or selective reconciliation. Claims 3–5 and 13–15.

164. In a vehicle computing environment, managing conflicts between distributed profile copies raises technical issues that do not arise in ordinary data-processing systems. The claims' requirement for conflict identification and reconciliation reflects a system-level solution for maintaining consistent vehicle configuration state across devices and vehicles.

165. The claims also require that profiles be structured using templates, including optional global standard templates common among vehicle manufacturers. Claims 9, 10, 19, and 20. From a technical perspective, these limitations impose structure on how vehicle configuration data is organized and shared, further distinguishing the claimed system from unstructured or ad hoc profile management.

166. Based on my review of the specification, the claims, and the Petition, I did not see evidence that this combination of vehicle-side authorization, authorization-first sequencing, vehicle-created authoritative profiles, and constrained synchronization with conflict handling was well-understood, routine, or conventional in passenger vehicle computing systems at the time of the invention.

167. In my technical opinion, from the perspective of a person of ordinary skill in the art, the inventive concept of the challenged claims resides in this ordered combination and system architecture, which improves how vehicle computing systems control access to, and modification of, vehicle configuration state.

168. I have reviewed the Petition and the Denning declaration with respect to their assertions that the challenged claims recite only well-understood, routine, and conventional activity. From a technical perspective, those assertions are not supported by evidence addressing the claimed system architecture in the context of passenger vehicle computing systems.

## **7. Technical Response to Assertions of Conventionality**

169. The Petition's analysis focuses primarily on whether individual components—such as verification, authentication, profile storage, or data transmission—were known in software systems generally. Pet. at 27–29. However, the claims do not merely recite these elements in isolation. They require a specific allocation of control, sequencing, and enforcement implemented by a vehicle computing system to govern vehicle operation.

170. In particular, the claims require that authorization to access and modify vehicle-stored profiles be determined by the vehicle system itself and that such authorization occur before any modification of vehicle-related preferences is determined or applied. Claims 1, 11. The Petition does not identify evidence showing that passenger vehicles conventionally implemented this authorization-first control architecture at the time of the invention.

171. The claims further require that updated user profiles governing vehicle operation be created at the vehicle. Claims 1, 11. External devices or servers may

receive transmitted copies of the profile, but they do not create the authoritative configuration state. The Petition does not cite prior vehicle systems, standards, or technical documentation showing that this vehicle-centric approach to profile creation and enforcement was routine or conventional.

172. The dependent claims also require identifying conflicts between vehicle-created profiles and profiles stored at other locations, and resolving those conflicts through overwriting or selective reconciliation. Claims 3–5 and 13–15. From a technical standpoint, managing conflicting configuration state across vehicles, devices, and servers presents challenges unique to vehicle systems, where inconsistent configuration can affect vehicle behavior and safety. The Petition does not identify evidence that passenger vehicles conventionally implemented such conflict identification and reconciliation mechanisms for vehicle configuration profiles.

173. The Denning declaration similarly does not establish conventionality in the relevant technical field. Mr. Denning’s analysis treats concepts such as verification, authentication, and data synchronization as generally known in software systems, without analyzing whether the claimed combination and control architecture were conventional in passenger vehicle computing systems. 1003 ¶¶ 132–135, 140–148.

174. From a technical perspective, this distinction matters. Vehicle computing systems operate under constraints and safety considerations that differ from those of general-purpose software systems. Architectural choices that may be common in other software contexts are not necessarily routine or conventional when applied to systems that directly control vehicle operation.

175. I did not see evidence in the Petition or the Denning declaration—such as contemporaneous vehicle architectures, industry standards, or widely deployed vehicle systems—showing that passenger vehicles at the time of the invention conventionally allocated authorization, enforcement, and profile creation to the vehicle in the manner required by the challenged claims.

176. Based on my review, the Petition’s assertions of conventionality rely on abstraction and generalization rather than on evidence demonstrating that the claimed ordered combination and vehicle-side control architecture were well-understood, routine, and conventional in the relevant technical field.

## **8. Summary of Technical Opinions Regarding Patent Eligibility**

177. In my technical opinion, from the perspective of a person of ordinary skill in the art, when the challenged claims are considered as a whole and in light of the specification, they are directed to a vehicle-side computing architecture that governs access to, and modification of, user profiles stored at the vehicle and associated with vehicle functions or settings. The claims define how authorization is

performed, when configuration changes are permitted, where updated profile state is created, and how that state is coordinated across distributed systems.

178. From the same technical perspective, the claims require vehicle-executed verification and/or authentication, an authorization-first sequence before any modification of vehicle-related preferences is determined or applied, and creation of updated user profiles at the vehicle to govern vehicle operation. These requirements reflect a concrete system design addressing technical issues that arise in computer-controlled vehicles, including unauthorized configuration changes, inconsistent system states, and loss of control over vehicle behavior.

179. It is also my technical opinion, from the perspective of a person of ordinary skill in the art, that the challenged claims recite an inventive concept. The inventive concept resides in the ordered combination of claim limitations that allocate authorization and enforcement to the vehicle, require authorization before any modification of vehicle settings, make the vehicle the authoritative source of configuration state, and constrain how vehicle-created profiles are propagated and reconciled across devices, servers, and other vehicles.

180. Based on my review, I did not see evidence in the Petition or the Denning declaration demonstrating that this ordered combination and vehicle-side control architecture was well-understood, routine, or conventional in passenger vehicle computing systems at the time of the invention. Assertions that individual

elements were known in software systems generally do not address whether the claimed architecture was conventional in the vehicle context.

**B. Ground 2: Claims 1, 6-8, 11, and 16-18 Would Not Have Been Obvious In View of Hendry.**

181. In my opinion, Hendry fails to render claims 1, 6-8, 11, and 16-18 obvious.

182. Claim 1 sets forth a system, whereas claim 11 sets forth a method. Claim 11 is substantially similar to claim 1 and the claims are addressed together below. Likewise, system claims 6-8 depend from claim 1 and are similar to method claims 16-18, which depend from claim 11. Accordingly, I will address claims 6 and 16; 7 and 17; and 8 and 18 together.

**1. Claims 1 and 11**

183. As I explained above, the steps of claims 1 and 11 are conditionally linked and performed in a required order, where later steps occur in response to an earlier authorization determination. The independent claims require receiving a request to access a user profile stored at a vehicle and determining, by performing a verification or authentication process in response to the request, whether the request is authorized to access the user profile, and in response to determining that the request is authorized to access the user profile, determining one or more requested modifications to stored preferences and creating an updated user profile.

184. In my opinion, Hendry fails to teach or suggest the following features, and therefore the Petition’s obviousness challenge based on Hendry fails to render claims 1 and 11 obvious.

- a. 1[c-1] receive a request to access a user profile stored at a vehicle, the user profile including one or more preferences associated with functions or settings of the vehicle;*

185. In my opinion, Petitioner and Mr. Denning fail to establish that Hendry teaches or suggests receiving a request to access a user profile stored at a vehicle. The only *received* request identified by Petitioner and Mr. Denning in Hendry is a request to establish a communications link between an external device and the vehicle. Petition at 41-44; Ex. 1003 at 165, 171, 173-174. Hendry’s Figures 3A, 3B, and 4B—which Petitioner and Mr. Denning rely upon and annotate—each expressly identify the received request as “Receive Request to Establish Communication [From/with] External Device.” Petition at 43-44; Ex. 1003 at 173-174; Ex. 1005 at Figures 3A-3B, 4B.

186. As explained above in Section VII.A, Hendry’s process indeed begins when an external device issues, and the vehicle receives, a request to establish a communications link, such as a Bluetooth pairing or synchronization request. Ex. 1005 ¶¶ 1, 4-5, 13, 17-18. The external device does not issue, and the vehicle does not receive, a request whose purpose is to access a user profile stored at the vehicle.

A request to establish communications seeks a different result than a request to access stored profile data.

187. Petitioner and Mr. Denning rely on Hendry’s statement that “[i]n essence, the user settings system 102 piggybacks the request to establish a communications link into a request to reinstate the personal settings of the user associated with the external device 100.” Petition at 41; Ex. 1003 at 170; Ex. 1005 ¶ 19. This passage does not teach receiving a request to access a user profile. Hendry explains that it is the vehicle’s user setting system, not the external device, that institutes the reinstatement of settings after the communications request has been authenticated. *Id.* ¶¶ 19-25. The request to reinstate the personal settings of the user is initiated, not received.

188. Hendry’s description confirms this sequence. The request to establish the communications link “will include the key of the external device 100 and a device identifier,” which the communication module verifies to determine the identity of the user or device and authenticate the device. *Id.* ¶ 18-19 (“the user settings system 10 uses a request from an external device 100 to establish the communications link to determine an identity of the user or the device”). Only after authentication does the system initiate retrieval of settings. *Id.* at 13, 19-25. The “piggybacked” reinstatement of settings is an operation automatically initiated by the vehicle after authentication, not a request that is received by the system.

189. Once Hendry determines the identity of the user (based on the request to establish a communications link) the communications module 104 transmits a signal to the vehicle modules to notify the user/device is in the vicinity of the vehicle (Ex. 1005 at ¶ 20) and in response to that notification, retrieving the settings (*id.* ¶¶ 21-25). In my opinion, a person of ordinary skill in the art would understand this notification signal is part of the internally initiated reinstatement process triggered after authentication, not a request received to access a user profile.

190. In my opinion, because the request for establishing a communications link is not a request to access a user profile, and because the separate process to reinstate settings is not received by Hendry's system, Petitioner has failed to prove that Hendry teaches or suggests "receive a request to access a user profile stored at a vehicle," as required by claims 1 and 11.

***b. 1[c-2] determine, by performing at least one of a verification process or an authentication process in response to the request, whether the request is authorized to access the user profile;***

191. In my opinion, Hendry also fails to teach or suggest element 1[c-2]: "determine, by performing at least one of a verification process or an authentication process in response to the request, whether the request is authorized to access the user profile."

192. As discussed above, Hendry does not disclose receiving a "request to access a user profile." As a result, Hendry necessarily does not disclose performing

verification or authentication in response to such a request. Even if Hendry's internal retrieval of settings were assumed to constitute the received request to access a user profile, which it does not, Hendry does not disclose performing any verification or authentication in response to that retrieval.

193. Hendry verifies or authenticates the external device only for the purpose of establishing a communications link. Ex. 1005 ¶ 31 ("the external device 100 will request to establish a communications link, and the communications module 104 will receive the request and verify and/or authenticate the external device 100."). Once authentication is complete, Hendry does not perform any further verification or authentication processes. Hendry expressly states that once a communications link is established, data is transferred freely between the external device and the vehicle. Ex. 1005 ¶ 15.

194. And only after the external device is verified/authenticated does Hendry's retrieval process begin. *Id.* ¶ 20 ("Once the external device 100 is verified/authenticated, the communications module 104 transmits a signal via a communication bus in the vehicle 10 to at least one of the HVAC module 108, the seat module 112, the A/V module 116, and the lighting module 120 notifying the modules that the external device 100 associated with the user is in the vicinity of the vehicle 10."), ¶¶ 21-25 (explaining retrieval of settings from various vehicle modules after receiving notification that user/device is in the vicinity of the vehicle).

195. In my opinion, a person of ordinary skill in the art would understand that Hendry's authentication establishes a trusted communications relationship, not permission to access protected profile data. Hendry does not treat stored settings as data whose access requires authorization. The authentication step is functionally exhausted once communications are established and is not reused or applied to govern access, or later modification or saving of settings.

196. Because Hendry fails to teach or suggest "determine, by performing at least one of a verification process or an authentication process in response to the request, whether the request is authorized to access the user profile" as set forth in claims 1 and 11, Hendry fails to render claims 1 and 11 obvious.

***c. 1[c-3] in response to determining that the request is authorized to access the user profile, determine, requested modifications to at least one of the one or more preferences; and***

197. Because Hendry fails to disclose receiving a request to access a user profile and fails to disclose authorization governing access to stored preferences, Hendry necessarily also fails to disclose determining requested modifications in response to authorized profile access. Hendry merely allows a user to change live vehicle settings and optionally save them, without determining those changes as requests to modify a user profile in response to authorization.

198. Figure 4B and paragraph 31 further confirm that Hendry does not authorize modification of stored settings. After the device is authenticated at step

354, the user may change vehicle settings “at any given time” (step 356) and may be prompted to save those settings (step 358). *Id.* ¶ 31, Figure 4B. Hendry does not disclose that saving modified settings is conditioned on authorization, verification, or any access-control decision. Once authentication for communications has occurred, Hendry permits modification and saving of settings without further authorization. *Id.*

199. Accordingly, Hendry fails to teach or suggest “in response to determining that the request is authorized to access the user profile, determine, requested modifications to at least one of the one or more preferences,” and thus fails to render obvious claim 1. Hendry fails to render obvious claim 11 for similar reasons.

200. Additionally, in my opinion, a person of ordinary skill in the art would not have been motivated to modify Hendry to arrive at the system recited in claim 1. The differences between Hendry and claim 1 are not matters of routine implementation or simple rearrangement of known steps, but instead reflect materially different system purposes and design choices.

201. Claim 1 is directed to managing authorized modification of a user profile stored at a vehicle. The claim requires that access to the user profile be subject to authorization, that requested modifications to profile preferences be determined only after authorization, and that an updated user profile be created in

response to those authorized modifications. This structure reflects a system in which stored preferences are treated as profile data whose modification is controlled.

202. Hendry addresses a different technical problem. Hendry is concerned with automatically restoring vehicle settings based on recognition of a previously paired external device. Ex. 1005 at Abstract, ¶¶ 1, 4, 5, 13, 31. Its verification and authentication processes are directed to establishing a trusted communications link between the vehicle and an external device. *Id.* After the authorization process has been completed, Hendry *assumes* that subsequent interactions, including changing and saving settings, are permitted. A person of ordinary skill in the art would understand that authentication is used for establishing a communications link, and Hendry does not disclose using it to authorize subsequent profile access/modification.

203. Hendry does not identify unauthorized modification of stored settings as a problem, and does not disclose any mechanism for controlling or restricting modification of stored preferences once a communication link has been established with the device. A person of ordinary skill in the art would understand that Hendry's architecture deliberately does not govern modification of stored settings through access control. In Hendry, verification and authentication are functionally exhausted once the communications link is established. Ex. 1005 ¶¶ 18-20, 27, 31, 33. After that point, the user may change vehicle settings at any given time, and the system

may save those changes if prompted. *Id.* ¶ 31. Hendry does not disclose performing any further authorization analysis to determine whether modification of stored preferences remains permitted.

204. A person of ordinary skill in the art would not have been motivated to repurpose Hendry's authentication mechanism to authorize modification of stored preferences. Hendry does not treat stored settings as protected profile data, and does not suggest that saving settings should be restricted once a trusted device is present. Modifying Hendry to implement authorization-controlled profile modification would require redesigning its data-control model rather than implementing an obvious variation.

205. Nor would a person of ordinary skill in the art understand Hendry to disclose or suggest a system in which authorization to modify stored profile data persists beyond the initial authentication event. Hendry authenticates an external device to establish a communications link and then assumes trust for subsequent operations, without describing authorization as a state that persists, is scoped, or is evaluated for purposes of modifying stored preferences.

206. Extending Hendry's initial authentication so that it authorizes modification of stored profile data for an indefinite period of time would require addressing significant system-design and security considerations that Hendry does not contemplate. For example, Hendry does not disclose whether authorization

would terminate upon loss of the communications link, vehicle shutdown, or user exit, or how the system would be prevented if control of the vehicle or device changes.

207. Hendry’s description that the system “piggybacks” a communications request to initiate restoration of settings would not have led a person of ordinary skill in the art to implement the system of claim 1. Hendry uses the term “piggybacking” to describe an internal operation in which the vehicle system initiates automatic restoration of previously stored settings after an external device has been authenticated or verified and allowed to establish a communication link, not a request to access a user profile. Treating Hendry’s piggybacking mechanism as a request to access and modify a user profile would require hindsight knowledge of the claimed invention.

208. The differences between Hendry and claim 1 cannot be bridged by merely changing the order of operations. Claim 1 requires a functional relationship in which authorization determines whether profile data may be accessed, and in which requested modifications and profile updates occur in response to that authorization. Hendry does not disclose or suggest that relationship.

209. Claim 1 addresses these differences by expressly tying authorization to profile access and by requiring that requested modifications and profile updates occur in response to that authorization. Hendry does not disclose this relationship

and does not provide a basis from which a person of ordinary skill in the art would arrive at it without hindsight reconstruction.

210. In my opinion, claims 1 and 11 are patentable.

## **2. Claims 6 and 16**

211. Claim 6 depends from claim 1, and claim 16 depends from claim 11. In my opinion, claims 6 and 16 are patentable for at least the reasons set forth below.

212. Claim 6 additionally requires that “the one or more processors are to perform both the verification process and the authentication process, and wherein the one or more processors are to determine that the request is authorized to access the user profile in response to successfully verifying the request via the verification process and successfully authenticating the request via the authentication process.”

213. As explained with respect to claim 1, Hendry does not disclose determining whether a request is authorized to access a user profile by performing either a verification process or an authentication process in response to such a request. Hendry therefore also fails to disclose the more specific requirement of claim 6, which requires that the system perform both verification and authentication and determine authorization to access the user profile only after both processes are successfully completed.

214. In Hendry, verification and authentication are performed solely to establish a communications link with an external device. E.g., Ex. 1005 ¶¶ 18–19,

33. Hendry does not disclose performing verification and authentication for the purpose of authorizing access to stored profile data, nor does it disclose determining authorization to modify stored preferences after both processes have been successfully completed. Once communications authentication is complete, Hendry permits modification and saving of settings without any further authorization analysis.

215. Accordingly, because Hendry does not teach or suggest determining that a request is authorized to access a user profile based on the successful completion of both a verification process and an authentication process, Hendry fails to teach or suggest the additional limitations of claim 6. Claim 16 is patentable for the same reasons, as it recites corresponding limitations in the method context.

### **3. Claims 7-8 and 17-18**

216. Claims 7-8 depend from claim 1, and claims 17-18 depend from claim 11. In my opinion, claims 7-8 and 17-18 are patentable for at least the reasons set forth below.

217. Claims 7 and 17 further limit the verification process recited in the independent claims by specifying how the verification process is performed. These claims presuppose the existence of a verification process that is used to determine whether a request is authorized to access a user profile stored at the vehicle.

218. As explained above with respect to claim 1, Hendry does not disclose performing any verification process to determine whether a request is authorized to access a user profile. Hendry's only verification-related activity is performed to authenticate an external device for purposes of establishing a communications link. E.g., Ex. 1005 ¶¶ 18–19, 33. Hendry does not disclose verifying a request to access profile data, nor does it disclose verification that governs access to or modification of stored user preferences.

219. Because Hendry does not disclose a verification process used to authorize access to a user profile at all, Hendry necessarily also fails to disclose the more specific verification techniques recited in claims 7 and 17. A person of ordinary skill in the art would not understand Hendry's device-pairing or communications-authentication mechanism to satisfy a verification process directed to authorizing profile access, as required by these claims.

220. Claims 8 and 18 further narrow the authentication process by specifying additional details regarding how authentication is performed. As explained above with respect to claim 1, Hendry does not disclose performing any authentication process to determine whether a request is authorized to access a user profile, and therefore does not disclose performing authentication in the particular manner recited in claims 8 and 18.

221. Accordingly, it is my opinion that Hendry fails to teach or suggest the additional limitations of claims 7–8 and 17–18, and that these claims are patentable over Hendry.

**C. Ground 3: Claims 2-7 and 12-17 Would Not Have Been Obvious over Hendry in View of Poulsen.**

222. In my opinion, Hendry in view of Poulsen fails to render claims 2-7 and 12-17 obvious.

223. Claims 2-7 depend from claim 1, and claims 12-17 depend from claim 11. These claims are similar in scope: claims 2-7 are system claims and 12-17 are corresponding method claims. I address claims 2 and 12; 3 and 13; 4 and 14; 5 and 15; 6 and 16; and 7 and 17 together.

224. I understand that Petitioner and Mr. Denning rely entirely on Poulsen (Ex. 1006) for the additional elements of claims 2-5 and 12-15. They do not contend that Hendry alone discloses, teaches, or suggests these additional elements. As a result, the asserted obviousness theory depends on an architectural rewrite, and Petitioner has not shown by a POSITA would do that.

225. Poulsen, however, addresses a fundamentally different technical problem than Hendry. Poulsen is directed to creating, storing, and sharing profiles across different environments and applications, such as documents, operating system configurations, or other content. Ex. 1006 ¶¶ 35, 82. Vehicles are merely one of many contemplated environments in Poulsen and are not central to its teachings.

Poulsen does not describe vehicle-resident user profiles accessed, modified, or controlled in response to authorization decisions, nor does it address profile management in connection with authenticated device presence in a vehicle, as required by the claims of the '243 patent.

226. Petitioner and Mr. Denning articulate a single, general motivation to combine Hendry and Poulsen, focused on transmitting, storing, and sharing of user profiles externally. Petition at 57-60; Ex. 1003 ¶¶ 308-318. That asserted motivation to combine, even if accepted, addresses only where profile data might be stored or shared. It does not address how or why a vehicle system would determine, whether conflicts exist between multiple instances of profile data, resolve such conflicts, or selectively update profile attributes as required by claims 3–5 and 13–15, performance of both a verification process and an authentication process as required by claim 6, or specific types of verification processes as required by claims 7. Neither the Petition nor Mr. Denning explains why a person of ordinary skill in the art would have been motivated to modify Hendry introduce conflict detection, overwriting of conflicted preferences, selective reconciliation, multiple or specific authentication/verification processes based on Poulsen.

227. Regarding claims 3-5 and 13-15 Poulsen itself does not describe conflict detection or conflict resolution logic, and does not use the term “conflict.” Instead, Poulsen describes prompting a user to decide whether to overwrite existing

profile data or selected attributes, in a manner analogous to a “Save As” function. Ex. 1006 ¶¶ 45, 47, 54, 57-58, 60-61, 63-64, 70-71, 83-84, 86-87.

228. Hendry does not identify conflicts between multiple stored profile instances as a technical problem that would motivate modification. In Hendry, user settings are stored in component-specific data stores and are retrieved or overwritten without any disclosure of maintaining multiple authoritative instances of a user profile whose contents could conflict. Nor does it suggest that resolving such conflicts is necessary or desirable. Absent any identified problem in Hendry relating to conflicting profile data, a person of ordinary skill in the art would have no reason to import Poulsen’s generalized profile-management concepts into Hendry.

229. In my opinion, Petitioner’s analysis of these claims reflects hindsight reconstruction. Petitioner’s repeatedly concludes that “[a] POSA would have understood the function of claim [3/4/5] would be performed by the one or more processors executing the machine readable instructions ... .” Petition at 68-71; Ex. 1003 ¶¶ 228, 232, 236. These statements begin with claimed function and then assert, without explanation, that the combined system would perform that function. This reasoning uses the challenged claims as a roadmap to reconstruct the invention, rather than identifying teachings or motivations in Hendry and Poulsen that would lead a person of ordinary skill in the art to implement the claimed features. Petitioner and Mr. Denning provide no additional analysis for claims 13-15 beyond

that same conclusory reasoning. It is my opinion that Hendry in view of Poulsen does not render claims 3–5 and 13–15 obvious.

230. Regarding claims 6 and 16, Petitioner and Mr. Denning argue in Ground 2 that Hendry includes processors to “perform ‘verify[ing] and/or authenticat[ing]’ to allow access to the associated user profile (i.e., one or both of a verification and authentication process).” Petition at 54-55; Ex. 1003 at 191. Petitioner and Mr. Denning then point to Poulsen’s discussions of authentication technologies “such as biometric identification (retinal scan, fingerprint, voice authentication, etc.), SmartCards, USB keys, etc.” Petition at 71; Ex. 1003 ¶ 238. Because Petitioner is not actually relying on Poulsen to modify Hendry for claim 6 or 16, there is no articulated combination rationale for those limitations, and where the features are already in Hendry, Poulsen adds nothing and cannot supply the missing ‘authorization-to-access-profile’ limitation.

231. This understanding is confirmed by Mr. Denning’s deposition testimony, in which he agreed that he was not proposing changes to Hendry based on Poulsen with respect to claim 6. Ex. 2023 at 112 (“Q: So would it be fair to say that with respect to Poulsen and claim 6, it discloses more of the same of what Hendry discloses, but you wouldn’t necessarily – you’re not proposing any changes to Hendry based upon Poulsen in your declaration? Is that a fair statement?” “A. That is fair.”). Because Hendry already discloses the relevant authentication

features, and because Petitioner has not articulated a reason to modify Hendry based on Poulsen to arrive at claims 6 and 16, Hendry in view of Poulsen does not render claims 6 and 16 obvious.

232. Regarding claims 7 and 17, Petitioner and Mr. Denning conclude that “Hendry in view of Poulsen likewise renders obvious claim 7 for the same reasons discussed for claim 6 (e.g., biometrics such as fingerprints).” Petition at 72; Ex. 1003 ¶ 240. As I explained above, Petitioner has not articulated a reason to modify Hendry based on Poulsen to arrive at claims 6 and 16, and so, Petitioner has also failed to articulate a motivation to modify Hendry based on Poulsen to arrive at the invention of claims 7 and 17. Accordingly, Hendry in view of Poulsen does not render claims 7 and 17 obvious.

### **1. Claims 2 and 12**

233. Claim 2 depends from claim 1, and claim 12 depends from claim 11. Claims 2 and 12 further limit the independent claims by adding additional requirements related to transmitting updated user profiles. For the reasons explained above with respect to claims 1 and 11, and because Hendry in view of Poulsen does not remedy the deficiencies identified with respect to those independent claims, it is my opinion that claims 2 and 12 are patentable.

## **2. Claims 3 and 13**

234. Claim 3 depends from claim 2, and claim 13 depends from claim 12. Claim 3 further requires “determine[ing] whether any conflicts exist between the updated preferences of the updated user profile and the local preferences of the local user profile.”

235. In my opinion, Poulsen fails to teach or suggest this additional feature of claim 3. Petitioner and Mr. Denning rely on a portion of paragraph 87 of Poulsen to assert that claim 3 would have been obvious. Petition at 67; Ex. 1003 ¶ 226. This portion of Poulsen describes prompting a user to confirm “whether the profile should be completely overwritten or if only the attributes selected for storage should be updated.” Ex. 1006 ¶ 87.

236. Although Poulsen describes prompting a user when saving profile data that may already exist, Poulsen does not describe determining whether any conflicts exist between updated preferences and existing local preferences. In my opinion, a person of ordinary skill in the art would rather understand Poulsen’s described mechanism as analogous to a “Save As” or overwrite confirmation function, which prompts a user to confirm whether to overwrite existing data regardless of whether any conflicting information exists.

237. Petitioner and Mr. Denning assert that “Poulsen discloses determining any changes made resulting in differences.” Petition at 67; Ex. 1003 ¶ 227. Neither

provides a citation supporting that assertion. Poulsen does not disclose comparing the contents of an existing profile with the contents of the to-be-saved profile to determine whether differences or conflicts exist. Instead, Poulsen only discloses prompting a user to confirm whether to overwrite existing data. Ex. 1006 ¶¶ 45, 47, 54, 57-58, 60-61, 63-64, 70-71, 83-84, 86-87.

238. As an illustrative example, a user could change a setting and later change it back, resulting in no difference between the current settings and the previously stored profile. Poulsen would still prompt the user to confirm whether to overwrite the stored profile purely based on its preexistence, demonstrating that Poulsen fails to teach or suggest “determine whether any conflicts exist between the updated preferences of the updated user profile and the local preferences of the local user profile.”

239. Poulsen never describes identifying conflicting preferences, comparing profile data to detect conflicts, or determining whether conflicts exist between updated and local preferences. Poulsen does not use the word “conflict” at all. Instead, Poulsen relies entirely on user confirmation to overwrite saved settings.

240. Because Poulsen fails to teach or suggest “determine[ing] whether any conflicts exist between the updated preferences of the updated user profile and the local preferences of the local user profile,” Hendry in view of Poulsen fails to render claim 3 obvious. Claim 13 is not obvious for the same reasons.

241. Additionally, as I explained previously, Petitioner has failed to articulate a motivation to modify Hendry based on Poulsen to arrive at the invention of claims 3 and 13, and instead relies on hindsight reconstruction.

### **3. Claims 4 and 14**

242. Claim 4 depends from claim 3, and claim 14 depends from claim 13. Petitioner and Mr. Denning rely on the same evidence for claims 4 and 14 as they do for claims 3 and 13. Claims 4 and 14 are patentable at least due to their dependency on these claims.

243. Because Hendry in view of Poulsen fail to teach or suggest “determining that one or more conflicts exist between the updated preferences and the local preferences” in claim 3, Hendry in view of Poulsen also necessarily fails to teach or suggest the additional limitation of claim 4: “in response to determining that one or more conflicts exist between the updated preferences and the local preferences, the one or more processors are to execute the machine-readable instructions to overwrite conflicted ones of the local preferences with corresponding conflicting ones of the updated preferences.” Accordingly, it is my opinion that claim 4 is patentable for the same reasons discussed above for claim 3, from which it depends. Claim 14 is patentable for similar reasons.

244. Additionally, Petitioner has failed to establish a motivation to combine Hendry and Poulsen to arrive at the invention of claims 4 and 14, and relies on hindsight reconstruction rather than teachings of the prior art.

#### **4. Claims 5 and 15**

245. Claim 5 depends from claim 3, and claim 15 depends from claim 13. Petitioner and Mr. Denning rely on the same evidence for claims 5 and 15 as they do for claims 3 and 13. Claims 5 and 15 are patentable at least due to their dependency on these claims.

246. Because Hendry in view of Poulsen fail to teach or suggest “determining that one or more conflicts exist between the updated preferences and the local preferences” as explained for claim 3, Hendry in view of Poulsen also fail to teach or suggest the additional elements of claim 5: “in response to determining that one or more conflicts exist between the updated preferences and the local preferences, the one or more processors are to execute the machine-readable instructions to perform a reconciliation process that allows selective determination of which conflicted ones of the local preferences should be overwritten by corresponding conflicting ones of the updated preferences.” Poulsen does not disclose a reconciliation process that selectively resolves conflicts between preferences. Instead, Poulsen discloses prompting a user to overwrite data without identifying conflicts or providing selective conflict resolution.

247. Petitioner has also failed to establish a motivation to combine Hendry and Poulsen to arrive at the invention of claims 5 and 15, and instead relies on hindsight reconstruction.

## **5. Claims 6 and 16**

248. Claim 6 depends from claim 1, and claim 16 depends from claim 11. Petitioner and Mr. Denning do not identify any aspects of Hendry that a person of ordinary skill in the art would be motivated to modify based on Poulsen to arrive at claims 6 and 16.

249. Indeed, as I explained previously, Petitioner has failed to articulate a motivation to modify Hendry based on Poulsen to arrive at the invention of claims 6 and 16.

250. Petitioner has additionally failed to establish the obviousness of these claims for the same reasons discussed above with respect to claims 6 and 16 in Ground 2.

## **6. Claims 7 and 17**

251. Claim 7 depends from claim 1, and claim 17 depends from claim 11. As explained above, Hendry does not disclose a verification process used to authorize access to or modification of a user profile, and Poulsen does not cure that deficiency. Poulsen's disclosure of authentication technologies does not relate to authorizing profile access or resolving conflicts between preferences.

252. And as I explained previously, Petitioner has failed to articulate a motivation to modify Hendry based on Poulsen to arrive at the invention of claims 7 and 17. Accordingly, Hendry in view of Poulsen fails to render claims 7 and 17 obvious.

**D. Ground 4: Claims 9-10 and 19-20 Would Not Have Been Obvious over Hendry in view of Rovik.**

253. In my opinion, Hendry in view of Rovik fails to render claims 9-10 and 19-20 obvious.

254. Claims 9-10 depend from claim 1, and claims 19-20 depend from claim 11. These claims are substantially similar in scope: claims 9-10 are system claims and claims 19-20 are corresponding method claims. I address claims 9 and 19 together, and claims 10 and 20 together.

255. Petitioner and Mr. Denning rely on Rovik (Ex. 1007) for the additional limitations recited in claims 9–10 and 19–20, rather than identifying those limitations in Hendry itself. In my opinion, this confirms that the asserted obviousness theory depends on importing features from Rovik into Hendry.

**1. Claims 9 and 19**

256. Claim 9 depends from claim 1, and claim 19 depends from claim 11. Claim 9 further requires that “the user profile is based on a template for the one or more preferences, and the updated user profile is created relative to the template.”

In my opinion, Petitioner and Mr. Denning error in equating Rovik’s disclosure with this claim language.

257. Petitioner asserts that Rovik discloses “example user profiles 510 and 512’ stored in a hard disk drive (HDD) in Figure 5 that include common setting options and common organization.” Petition at 76-77; Ex. 1003 ¶ 255. Then, Petitioner argues that Rovik’s user profiles 510 and 512 “could readily be transferred and applied to a new vehicle or vehicle type.” Petition at 78; Ex. 1003 ¶ 258. In my opinion, that analysis does not establish that a person of ordinary skill in the art would have been motivated to modify Hendry to implement the templated, vehicle-resident user-profile functionality recited in claim 9.

258. Petitioner’s assertion that Rovik’s profiles “could readily be transferred and applied” does not supply a motivation to combine. Petitioner at 103. A showing that something could be done is not the same as explaining why a person of ordinary skill would have been motivated to alter Hendry’s in-vehicle, component-module architecture to implement Rovik’s server-centered profile framework, or why such a modification would have been expected to succeed in the manner required by claims 9–10.

259. Hendry is designed around reinstating settings for a single vehicle by authenticating a paired external device and then retrieving locally stored parameters from data stores. Hendry’s system architecture is local and distributed within the

vehicle. Hendry does not address cross-vehicle portability, remote-server computation, or translation of user attributes into different vehicle-specific outputs.

260. Rovik explains that different vehicles may have different adjustable components, different available options, and different capabilities, even among vehicles of the same model. Ex. 1007 at 7:48-59, 8:7–10, 8:32–39, 8:55–59. Rovik therefore teaches that the settings applicable in one vehicle may not map directly to another vehicle, including where a second vehicle lacks automatically adjustable components (e.g., manual seats, mirrors, or pedals). *Id.* at 8:32–39, 8:55–59.

261. For vehicles that a user has never used before, Rovik describes a process performed by a remote server to generate new user settings. *Id.* at 9:14-17; 10:6–16; 13:2–6. Rovik explains that “generating a new user setting can involve using a user attribute in the user profile ... in combination with a vehicle attribute in the vehicle profile ... to calculate a user setting for a position of a component.” *Id.* at 13:2–6. Rovik then transmits the calculated settings to the vehicle. *Id.* at 13:10–13; Fig. 9 (steps 720–722).

262. Rovik addresses a different design problem than Hendry and adopts a different architectural solution. Rovik recognizes that different vehicles have different geometries, adjustable components, and capabilities—including within a single model—and it therefore stores user attributes and vehicle profiles at a remote server and calculates vehicle-specific settings for new vehicles the user has never

driven. Ex. 1007 at 8:7–10, 8:32–39, 8:55–59; 9:54–57; 10:6–16; 13:2–13. In Rovik, the “standard vehicle” and “standardized” user profile are used as a computational reference at the server, not as a vehicle-resident template for storing and updating a user profile.

263. For that reason, a person of ordinary skill in the art would not be motivated to modify Hendry to “transfer” Rovik’s standardized user profile to the vehicle and use it as a template for creating and updating a vehicle-resident user profile. Rovik’s standardization is expressly tied to server-side generation of new vehicle-specific settings based on a combination of user attributes and vehicle profiles. Ex. 1007 at 9:14–10:25; 13:2–13. Importing that concept into Hendry would not naturally yield the templated, vehicle-resident profile creation and update mechanisms recited in claim 9, because Rovik does not use its standardized profile at the vehicle to structure or update stored profile preferences.

264. Rovik’s emphasis on vehicle-specific constraints undermines the premise that a single standardized profile is suitable for direct application at a vehicle as a common template. Rovik explains that settings may not map directly where a target vehicle lacks particular automatically adjustable components or has different system availability and capabilities. Ex. 1007 at 8:32–39, 8:55–59. A person of ordinary skill would therefore understand that direct profile transfer, without server-side translation and vehicle-profile constraints, would not reliably produce usable or

correct settings from each profile field in a new vehicle. Because Rovik teaches that direct transfer is unreliable and requires server-side translation, a POSITA would not have been motivated to apply Rovik's profiles as a vehicle-resident template in Hendry, and Rovik in fact teaches away from such a modification.

265. Petitioner also lacks a coherent implementation pathway that would integrate Rovik's server-side vehicle-profile computation with Hendry's in-vehicle component-module datastores in a way that yields a "user profile stored at a vehicle" that is "based on a template," with updates "created relative to the template." Hendry would have to be redesigned to (i) store profile data at the vehicle in a templated structure, (ii) maintain that template structure during update operations, and (iii) reconcile that structure with vehicle-specific feature availability that Rovik treats as a server-side constraint. Neither Petitioner nor Mr. Denning explains why a person of ordinary skill would undertake that redesign, likely due to misunderstanding Rovik's teachings, as opposed to following Rovik's approach of generating vehicle-specific settings at a server and transmitting those settings to the vehicle.

266. In my opinion, these architectural and functional differences are not superficial. They reflect different assumptions about where profile intelligence resides (vehicle modules versus remote server), what is being transferred (raw settings versus computed vehicle-specific outputs), and how variability across vehicle models is handled (local storage versus server-side vehicle profiles).

Because Petitioner has not articulated technical reason to replace Hendry's local reinstatement system with Rovik's server-side translation system, and to do so in a way that results in a vehicle-resident templated profile, Petitioner has not shown a motivation to combine that would lead a person of ordinary skill to arrive at the claimed invention.

267. In this architecture, Rovik's "standardized" user profile is not a template for preferences common among vehicles, nor is it disclosed as a template that is used at vehicles to structure to store or update profile data. Rather, as discussed above, Rovik standardization is a server-side construct used to generate different vehicle-specific settings for vehicles in view of vehicle geometry and capability constraints. Ex. 1007 at 9:14-10:25; 13:2-6. This architectural choice explains why a person of ordinary skill in the art would not have been motivated to modify Hendry to store or update a templated user profile at the vehicle based on Rovik's teachings.

268. For these reasons, and consistent with the architectural and motivational analysis above, Rovik's disclosure is inconsistent with the requirement of claim 9 that the user profile stored at the vehicle is "based on a template" and that the updated user profile is "created relative to the template." Rovik does not describe storing at the vehicle a templated user profile that is updated relative to a template. Instead, Rovik teaches generating vehicle-specific settings at a remote

server based on user and vehicle profiles maintained at the server, and then transmitting just the resulting settings to a vehicle. Ex. 1007 at 9:14-10:25; 12:50-13:13.

269. In addition, Petitioner’s suggestion that Rovik’s user profiles “could readily be transferred and applied” (Petition at 78) does not establish that a person of ordinary skill in the art would modify Hendry to transfer Rovik’s standardized user profiles to a vehicle and use them as a template for creating an updated user profile. Rovik teaches away from direct transfer of such profiles by emphasizing vehicle-specific geometry and capability constraints, and by expressly generating new, vehicle-specific settings for transmission. Ex. 1007 at 8:32–39; 8:55–59; 9:14-17; 9:40-43; 9:54-64; 12:50-13:13.

270. More fundamentally, Rovik’s transmitted output is described as one or more user settings for vehicle components (e.g., seat position), calculated by the server for a particular vehicle. Ex. 1007 at 13:2–13. Rovik does not describe transmitting a vehicle-resident user profile data structure that includes an association to a user and a templated organization of multiple preferences, as recited in claim 9.

271. The ’243 patent describes user profiles as stored data structures associated with a user identity and including preferences or settings for vehicle functions. Ex. 1001 at 57:65–58:20; 58:35–47; 59:49–64; Figures 12A-12D. The claims likewise recite that the user profile includes “one or more preferences

associated with functions or settings of the vehicle.” Ex. 1001, claims 1 and 11. In my opinion, transmitting calculated vehicle-specific settings to a vehicle, without more, does not teach or suggest a user profile stored at the vehicle that is based on a template and updated relative to that template.

272. It is also anticipated that the profile identification module may communicate with other components to load preferences, settings, and/or conditions based on the user profile. Ex. 1001 at 44:23–27. This disclosure is consistent with the concept that a profile stored at the vehicle serves as a structured repository of user-specific preferences that the vehicle can access and update.

273. For at least these reasons, Hendry in view of Rovik fails to teach or suggest the templated, vehicle-resident user profile limitation recited in claim 9. Accordingly, it is my opinion that claim 9 is not rendered obvious by Hendry in view of Rovik. Claim 19 is not rendered obvious for similar reasons.

274. In addition, and independent of the foregoing, Hendry in view of Rovik is not relied upon to, and does not cure the deficiencies discussed above with respect to claims 1 and 11. Because claims 9 and 19 depend from those independent claims, Hendry in view of Rovik likewise fails to render claims 9 and 19 obvious.

## **2. Claims 10 and 20**

275. Claim 10 depends from claim 9, and claim 20 depends from claim 19. Claim 10 further requires that “the template is a global standard template that is

common among at least two vehicle manufacturers.” In my opinion, the same misunderstanding of Rovik that underlies Petitioner’s analysis of claim 9 applies with equal force to claim 10.

276. Petitioner again argues that “Rovik discloses ‘example user profiles 510 and 512’ stored in an HDD in Figure 5 that include common setting options and common organization that were standardized to apply to a standard vehicle.” Petition at 79. Petitioner then argues that:

Rovik discloses the user profiles are intended to be applied to “vehicles of different makes and models,” EX1007, 2:1-5, and various “types of vehicles,” e.g., “passenger automobiles,” “trucks”, “boats,” etc. EX1007, 3:20-31; EX1003 ¶¶263, 109, including a “different vehicle [that] is unfamiliar to the driver, such as a rental car that is a different make or model from the user’s usual vehicle....” EX1007, 1:25-32; EX1003 ¶¶263, 109.

*Id.* at 80.

277. Rovik’s discussion of different vehicle types, however, does not teach or suggest a global standard template that is common among at least two vehicle manufacturers. Rather, Rovik explains that vehicles differ in geometry, component availability, and system capabilities, and that these differences must be accounted for when determining appropriate settings. Ex. 1007 at 8:7–10, 8:32–39, 8:55–59;

10:6–16. Rovik therefore teaches generating different vehicle-specific settings for different vehicles, not applying a single common template across vehicles from different manufacturers.

278. As explained above with respect to claim 9, Rovik’s “standardized” user profiles are stored and used at a remote server as a reference model to facilitate calculation of new, vehicle-specific settings. Ex. 1007 at 9:14–10:25; 13:2–6. Rovik combines user attributes with vehicle-specific profiles to generate settings tailored to a particular vehicle’s geometry and capabilities, and then transmits those calculated settings to the vehicle. *Id.* at 9:14-10:25; 12:50-13:13. Rovik does not disclose transmitting a templated user profile to vehicles, let alone a template that is global and common among at least two vehicle manufacturers.

279. Because Rovik’s approach depends on generating vehicle-specific settings rather than applying a global standard template across different manufacturers, Hendry in view of Rovik fails to teach or suggest the limitation of claim 10. Accordingly, in my opinion, claim 10 is not rendered obvious by Hendry in view of Rovik. Claim 20 is not rendered obvious for similar reasons.

**E. Ground 5: Claims 1, 6-7, 11, and 16-17 Would Not Have Been Obvious over Singh.**

**1. Claims 1 and 11**

- a. 1[c-1] receive a request to access a user profile stored at a vehicle, the user profile including one or more preferences associated with functions or settings of the vehicle;*

280. In my opinion, Petitioner and Mr. Denning fail to prove that Singh teaches or suggests “receive a request to access a user profile stored at a vehicle, the user profile including one or more preferences associated with functions or settings of the vehicle,” as required by claims 1 and 11.

281. Petitioner and Mr. Denning assert that Singh discloses “a multi-factor authentication/verification process to initiate a request to access a user profile stored at the vehicle.” Petition at 83; Ex. 1003 ¶ 284. However, neither Petitioner nor Mr. Denning clearly identify any structure, signal, message, or operation in Singh that constitutes a request to access a user profile. Rather, both Petitioner and Mr. Denning merely conclude that such a request is *initiated*.

282. Singh describes a sequence in which a driver enters a password, scans a fingerprint, and—only after successful verification and vehicle entry—triggers a Features Loading Program that loads stored vehicle settings. Ex. 1008 ¶¶ 39–41. Singh does not describe the driver or any component of the system issuing a request to access a user profile, nor does it describe the system receiving such a request. The

Features Loading Program is an internally initiated process that follows authentication and vehicle entry, not a received request to access a user profile.

283. Initiating a process after authentication is not the same as receiving a request to access a user profile. Claims 1 and 11 require that the system receive a request whose purpose is to access a user profile. Singh does not disclose such a request, either explicitly or implicitly.

284. Petitioner and Mr. Denning fail to establish that Singh teaches or suggests “receive a request to access a user profile stored at a vehicle, the user profile including one or more preferences associated with functions or settings of the vehicle” as required by claim 1.

***b. 1[c-2] determine, by performing at least one of a verification process or an authentication process in response to the request, whether the request is authorized to access the user profile;***

285. In my opinion, Singh fails to teach or suggest “determine[ing], by performing at least one of a verification process or an authentication process in response to the request, whether the request is authorized to access the user profile,” as required by claims 1 and 11.

286. Limitation 1[c-2] is dependent on limitation 1[c-1]. It requires that verification or authentication be performed *in response to* a request to access a user profile. As explained above, Petitioner and Mr. Denning have failed to identify any

request to access a user profile in Singh. In the absence of such a request, Singh cannot disclose performing verification or authentication in response to it.

287. Petitioner and Mr. Denning assert that Singh’s multi-factor authentication/verification process *initiates* a request to access a user profile stored at the vehicle for element 1[c-1]. Petition at 83; Ex. 1003 ¶ 284; Paper 7 at 35. But under that theory, Singh necessarily fails to teach or suggest “performing at least one of a verification process or an authentication process *in response to the request*” because the authentication and verification processes would precede the request rather than be performed in response to it. This sequencing is consistent with Singh’s disclosure that passwords and fingerprint verification occurs first, and only after successful verification does the system initiate a “Features Loading Program” to access and apply user settings. Singh’s Features Loading Program is initiated only “[o]nce the verification has been performed and the vehicle started.” Ex. 1008 ¶ 41. Even if the Features Loading Program were construed as accessing user profile data, Singh does not teach or suggest any authentication or verification process in response to the Features Loading Program. Nor do Petitioner and Mr. Denning identify any other operation in Singh that could constitute a request to access a user profile followed by responsive verification or authentication.

288. In my opinion, Singh does not teach or suggest “determine[ing], by performing at least one of a verification process or an authentication process in

response to the request, whether the request is authorized to access the user profile,” as required by claims 1 and 11.

- c. 1[c-3] in response to determining that the request is authorized to access the user profile, determine, requested modifications to at least one of the one or more preferences; and*

289. Because Singh fails to disclose receiving a request to access a user profile and fails to disclose authorization governing access to stored preferences, Singh necessarily also fails to disclose determining requested modifications in response to authorized profile access. Singh merely allows a user to change live vehicle settings, optionally save them, or save them when the vehicle is turned off, without determining those changes as requested modifications to a user profile in response to determining that a request to access the user profile is authorized, as required by the claims. Ex. 1008 ¶¶ 62-64.

290. Similar to my explanation above for claims 1 and 11 in Ground 2, Singh *assumes* that interactions subsequent to its fingerprint and password processes, including changing and saving settings, are permitted. A person of ordinary skill in the art would understand that authentication is used for establishing vehicle entry, and Singh does not disclose using it to authorize subsequent profile access/modification. A person of ordinary skill in the art would not have been motivated to repurpose Singh’s authentication/verification mechanism to authorize modification of stored preferences.

291. In my opinion, a person of ordinary skill in the art would not have been motivated to modify Singh to arrive at the system recited in claims 1 and 11. Singh reflects a deliberate design choice in which authentication and verification are used exclusively to control vehicle entry and operation, not as mechanisms for authorizing access to or modification of stored user profile data.

292. Singh is focused on unauthorized vehicle use. Ex. 1008 ¶¶ 2–4. To address those concerns, Singh requires successful completion of a password entry and fingerprint scan before unlocking the vehicle and starting the engine. Only after the vehicle is opened and started does Singh initiate its Features Loading Program to load stored preferences. Ex. 1008 ¶¶ 39–41. Singh does not describe authentication as governing subsequent access to profile data, nor does it treat profile access as a security-controlled operation.

293. Once Singh’s authentication steps are completed and the vehicle is started, Singh assumes that subsequent interactions are permitted, including changing settings and saving those changes. Ex. 1008 ¶ 62. Singh does not disclose performing any additional authorization analysis before allowing changes to stored preferences, nor does it describe any mechanism for evaluating whether a request to modify a user profile remains authorized after the vehicle has been opened.

294. A person of ordinary skill in the art would understand that Singh’s authentication is functionally exhausted once the driver is authenticated and granted

access to operate the vehicle. Singh does not describe authorization as a state that is evaluated in connection with accessing or modifying stored profile data. Modifying Singh to implement request-based authorization of profile access would therefore require introducing a new access-control mechanism that Singh neither discloses nor suggests.

295. Nor does Singh identify any technical problem associated with unauthorized modification of stored profile data that would motivate such a modification. Singh allows drivers to change and save settings through a graphical user interface, and even automatically saves changes when the vehicle is turned off. Ex. 1008 ¶ 62. Singh's silence regarding authorization of profile modification reflects a design assumption that such modifications do not require separate access control once the driver has been authenticated to use the vehicle.

296. Accordingly, a person of ordinary skill in the art would not have been motivated to repurpose Singh's password and fingerprint authentication mechanisms to authorize requests to access or modify a user profile, as required by claims 1 and 11. Doing so would require redesigning Singh rather than implementing an obvious or routine variation of Singh's disclosed system.

297. Accordingly, it is my opinion that claim 1 is not rendered obvious by Singh. Claim 11 is not rendered obvious by Singh for similar reasons.

## **2. Claims 6 and 16**

298. Claim 6 depends from claim 1, and claim 16 depends from claim 11. Claims 6 and 16 further require determining that a request is authorized to access a user profile in response to successfully performing both a verification process and an authentication process. As explained above, because Singh fails to teach or suggest the limitations of the independent claims, Singh likewise fails to render claims 6 and 16 obvious.

## **3. Claims 7 and 17**

299. Claim 7 depends from claim 1, and claim 17 depends from claim 11. Claims 7 and 17 further specify types of verification processes. As explained above, because Singh fails to teach or suggest the limitations of the independent claims, Singh likewise fails to render claims 7 and 17 obvious.

### **F. Ground 6: Claims 2-8 and 12-18 Would Not Have Been Obvious over Singh in view of Cazanias and Forstall.**

300. In my opinion, Singh in view of Cazanias and Forstall fails to render claims 2-8 and 12-18 obvious.

301. Claims 2-8 depend from claim 1, and claims 12-18 depend from claim 11. These claims are substantially similar in scope: claims 2-8 are system claims and 12-18 are corresponding method claims. I address claims 2 and 12; 3 and 13; 4 and 14; 5 and 15; 6 and 16; 7 and 17; and 8 and 18 together.

302. As an initial matter, Petitioner and Mr. Denning rely on Cazanias (Ex. 1009) and/or Forstall (Ex. 1010), rather than Singh for the additional limitations recited in claims 2-5, 8, 12-15, and 18. Singh itself does not disclose those additional features. The asserted obviousness theory therefore depends on importing teachings from Cazanias and Forstall into Singh.

303. Petitioner and Mr. Denning set forth a generic motivation to combine Singh, Cazanias, and Forstall, focused exclusively on transmitting and saving user profiles to an external location. Petition at 89 (e.g., “a POSA would have been motivated to transmit and save profiles to an external location (such as to a server, mobile device, database, etc.) for various purposes ...”); Ex. 1003 ¶¶ 308-318 (e.g., “a POSITA would also have been motivated to transmit and save profiles to an external location (such as to a server, mobile device, database, etc.) for various purposes ...”). This asserted motivation is substantially similar to the motivation advanced for the Hendry–Poulsen combination, which, as I explained above, does not address the additional limitations relating to conflict determination and reconciliation.

304. Neither the Petition nor Mr. Denning’s declaration explains why a person of ordinary skill in the art would be motivated by Forstall to modify Singh and Cazanias in way that satisfies the additional elements of claims 3-5 and 13-15,

which relate to determining whether conflicts exist and reconciling conflicting preferences.

305. In fact, Singh, Cazanias, and Forstall are directed to fundamentally different technical problems, operating at different layers of the system stack and employing materially different architectural assumptions and mechanisms. Singh is concerned with local driver identification for purposes of controlling vehicle access and operation, followed by reinstatement of a vehicle profile stored locally within the vehicle. E.g., Ex. 1008 ¶ 4. Cazanias, in contrast, addresses centralized, server-based portability of driver profiles across multiple vehicles, relying on telematics units and backend infrastructure to store and distribute driver profile data. E.g., Ex. 1009 at 6:13-34. Forstall addresses an entirely different problem space—namely, bidirectional synchronization of general data items between a mobile device and a vehicle device, such as navigation information and contact data, with user-defined synchronization and conflict-resolution settings. E.g., Ex. 1010 at Abstract, ¶¶ 13, 79-80, 90. As a result, these references do not disclose compatible or “complementary” teachings, as asserted by Petitioner. Instead, they reflect architecturally disparate systems designed to achieve distinct objectives, and a person of ordinary skill in the art would have had no technical basis or motivation to combine them in the manner proposed.

306. Petitioner offers no art-based rationale explaining why a person of ordinary skill in the art would have looked to Forstall’s mobile-device synchronization framework to modify either Singh’s vehicle access-control and local profile-reinstatement system or Cazan’s server-centric profile portability architecture. Forstall is notably unconcerned with secure access to vehicle-stored user profiles or with authorizing requests to access such profiles. Instead, it merely permits user-initiated synchronization and reconciliation of general data. E.g., Ex. 1010 ¶¶ 90-91. Petitioner’s proposed combination thus relies on impermissible hindsight driven by the challenged claims, not a technical motivation rooted in the prior art.

307. I understand that Petitioner’s reliance on generalized assertions that the references are in the “same field” is technically insufficient as obviousness requires an explanation as to why and how a person of ordinary skill in the art would combine specific teachings of Singh, Cazan, and Forstall in the manner claimed with a reasonable expectation of success. Petitioner fails to explain *why* a person of ordinary skill in the art attempting to improve Singh’s vehicle-based profile management would look to Forstall’s device-to-device synchronization techniques to modify a system focused on authorization for vehicle access, operation, and loading of user-specific settings.

308. Petitioner also fails to explain *how* a person of ordinary skill in the art would actually combine these three references into a single, coherent system or method. Rather than analyzing the prior art as complete technical systems, Petitioner abstracts individual components from each reference and recombines them as if they were modular and interchangeable, but they are not modular due to architectural dependencies, execution flows, and system-level constraints that would dictate how any such combined system could actually operate.

309. Petitioner further fails to explain how a person of ordinary skill in the art *would have reasonably expected success* in combining these systems without fundamentally altering their architectures. Singh is premised on reinstating locally stored settings after a driver has already been authenticated for vehicle access and operation. Cazanas relies on remote storage and retrieval of profiles via telematics infrastructure. Forstall is designed for bidirectional synchronization between independent devices using user-controlled conflict-resolution rules. These materially different design premises undermine any reasonable expectation that the systems could be integrated as proposed.

310. This is evident in Petitioner's lack of any specificity regarding which system properties or method steps are retained from Singh, which are purportedly incorporated from Cazanas and at what point in Singh's process, and which

additional properties or steps are taken from Forstall to fit into the unarticulated combination of Singh and Cazanias.

311. Petitioner provides no explanation as to how Singh’s locally stored vehicle user profile would be modified to incorporate Cazanias’s server-based profile transfer mechanisms. Petitioner further provides no explanation as to how Forstall’s mobile-device synchronization and conflict-resolution framework would be integrated into either Singh’s or Cazanias’s systems without fundamentally altering their operation. Petitioner also provides no explanation as to how these disparate teachings would be combined while still performing the claimed steps in the required order, including authorizing access to a vehicle-stored user profile in response to a request before determining requested modifications and creating an updated profile.

312. In my opinion, Petitioner’s analysis of these claims relies heavily on hindsight reconstruction. For claims 3-5, Petitioner repeatedly concludes “[a] POSA would have understood the function of claim [3/4/5] would be performed by the one or more processors executing the machine readable instructions ...” Petition at 96-97; Ex. 1003 at ¶¶ 333, 335, 338. This reasoning begins with the claimed function and then asserts, without explanation, that the combined system would perform that function. Petitioner and Mr. Denning provide no articulated reasoning grounded in the teachings of Singh, Cazanias, or Forstall explaining how or why those references would be combined to achieve the claimed functionality.

313. Because Petitioner and Mr. Denning fail to articulate a motivation to combine Singh, Cazanias, and Forstall to address the additional limitations of claims 3–5 and 13–15, fail to establish a reasonable expectation of success in such a combination, and rely on hindsight reconstruction rather than teachings of the prior art, it is my opinion that Petitioner has failed to prove obviousness of at least claims 3–5 and 13–15.

**1. Claims 2 and 12**

314. Claim 2 depends from claim 1, and claim 12 depends from claim 11. For the reasons discussed above with respect to claims 1 and 11, and because Singh in view of Cazanias and Forstall does not remedy the deficiencies identified in those independent claims, it is my opinion that claims 2 and 12 are not rendered obvious.

**2. Claims 3 and 13**

315. Claim 3 depends from claim 2, and claim 13 depends from claim 12. In my opinion, claims 3 and 13 are patentable at least due to their dependency on their respective patentable independent claims.

316. As I explained above, Petitioner has failed to articulate a motivation to modify Singh using the teachings of Cazanias and Forstall to arrive at the conflict-determination functionality recited in claims 3 and 13, and instead relies on hindsight reconstruction. Accordingly, it is my opinion that claims 3 and 13 are not rendered obvious.

### **3. Claims 4 and 14**

317. Claim 4 depends from claim 3, and claim 14 depends from claim 13. In my opinion, claims 4 and 14 are patentable at least due to their dependency on their respective patentable independent claims.

318. Because Singh in view of Cazanar and Forstall fails to teach or suggest determining that conflicts exist, as required by claims 3 and 13, the combination likewise fails to teach or suggest the additional limitations of claims 4 and 14. For the same reasons discussed above, Petitioner has failed to establish a motivation to combine or avoid hindsight reconstruction. Claims 4 and 14 are therefore not rendered obvious.

### **4. Claims 5 and 15**

319. Claim 5 depends from claim 3, and claim 15 depends from claim 13. In my opinion, claims 5 and 15 are patentable at least due to their dependency on their respective patentable independent claims.

320. As explained above, neither Singh nor the asserted combination with Cazanar and Forstall teaches or suggests determining conflicts or performing selective reconciliation of conflicting preferences. Petitioner has not articulated why a person of ordinary skill in the art would combine these references to arrive at the claimed reconciliation process. Accordingly, claims 5 and 15 are not rendered obvious.

## **5. Claims 6 and 16**

321. Claim 6 depends from claim 1, and claim 16 depends from claim 11. In my opinion, claims 6 and 16 are patentable at least due to their dependency on their respective patentable independent claims.

322. Similar to Petitioner's failures analyzing these claims in Ground 3, Petitioner and Mr. Denning do not identify any aspect of Singh that would be modified using Cazanias or Forstall to arrive at authorization-related claims 6 and 16. Instead, Petitioner points to authentication mechanisms allegedly disclosed in both Singh and Cazanias. Where Singh already discloses the asserted authentication features, a person of ordinary skill in the art would not be motivated to combine Cazanias for duplicative teachings.

323. For similar reasons discussed above with respect to claims 6 and 16 in Ground 3, and because Petitioner has failed to articulate a motivation to combine or avoid hindsight reconstruction, Singh in view of Cazanias and Forstall does not render claims 6 and 16 obvious.

## **6. Claims 7-8 and 17-18**

324. Claims 7-8 depend from claim 1, and claims 17-18 depend from claim 11. In my opinion, claims 7-8 and 17-18 are patentable at least due to their dependency on their respective patentable independent claims.

**G. Ground 7: Claims 9-10 and 19-20 Would Have Been Obvious over Singh in view of Rovik.**

325. In my opinion, Singh in view of Rovik fails to render claims 9-10 and 19-20 obvious.

326. As in Ground 4, Petitioner and Mr. Denning rely on Rovik (Ex. 1007), rather than Singh, for the additional limitations recited in claims 9–10 and 19–20. Singh itself does not disclose the templated user-profile features required by these claims. The asserted obviousness theory therefore depends on incorporating Rovik’s teachings into Singh.

**1. Claims 9 and 19**

327. Claim 9 depends from claim 1, and claim 19 depends from claim 11. In my opinion, claims 9 and 19 are patentable at least due to their dependency on their respective patentable independent claims.

328. Petitioner’s arguments for Ground 7 with respect to claims 9 and 19 mirror its arguments for Ground 4. As explained above, Rovik does not disclose or suggest a vehicle-resident user profile based on a template, nor does Rovik disclose creating an updated user profile relative to such a template. Instead, Rovik teaches generating vehicle-specific settings at a remote server and transmitting those settings to a vehicle. For the same reasons discussed in Ground 4, Singh in view of Rovik fails to render claims 9 and 19 obvious.

## **2. Claims 10 and 20**

329. Claim 10 depends from claim 9, and claim 20 depends from claim 19. In my opinion, claims 10 and 20 are patentable at least due to their dependency on their respective patentable independent claims.

330. Petitioner's arguments for Ground 7 with respect to claims 10 and 20 likewise mirror its arguments for Ground 4. As explained above, Rovik does not disclose or suggest a global standard template common among at least two vehicle manufacturers. Rovik's "standardized" profiles are server-side reference models used to generate vehicle-specific settings, not global templates applied across different manufacturers. Accordingly, for the same reasons discussed in Ground 4, Singh in view of Rovik fails to render claims 10 and 20 obvious.

## **IX. CONCLUSION**

331. In my opinion, claims 1-20 of the '243 Patent are (1) directed to patent-eligible subject matter and (2) are not rendered obvious by Hendry, Hendry in view of Poulsen, Hendry in view of Rovik, Singh, Singh in view of Cazanias and Forstall, or Singh in view of Rovik. Accordingly, it is my opinion that claims 1-20 are all patentable.

332. In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to

cross-examination. If cross-examination is required of me, I will appear for cross-examination at a mutually agreeable time and date within the United States during the time allotted for cross-examination.

333. I declare that all statements made herein of my knowledge are true and correct. I also declare 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 35 U.S.C. § 1001.

334. I declare under the penalty of perjury that the foregoing is true and correct.

Executed on: January 9, 2026

A handwritten signature in black ink, appearing to read 'Paul D. Martin', written above a horizontal line.

---

Paul D. Martin, Ph.D.