

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

PATENT OWNER'S RESPONSE

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE '243 PATENT	2
III.	SUMMARY OF THE ASSERTED REFERENCES	5
	A. Hendry	6
	B. Poulsen.....	8
	C. Rovik	10
	D. Singh.....	12
	E. Cazanass.....	14
	F. Forstall.....	15
IV.	GROUND 1: THE CHALLENGED CLAIMS ARE PATENT ELIGIBLE UNDER 35 U.S.C. § 101.....	17
	A. Alice Step One: The Claims Are Directed to a Vehicle-Side Computing Architecture That Improves the Operation and Security of Vehicle Computing Systems.	18
	1. The Claims Define a Vehicle-Side Control Architecture Governing Access to and Modification of Vehicle Settings.	20
	2. The Petition's Step-One Framing Improperly Abstracts Away the Claimed Vehicle-Side Control Architecture.....	26
	B. Even If the Board Were to Proceed to Alice Step Two, the Claims Recite an Inventive Vehicle-Side Control Architecture That Was Neither Routine nor Conventional.	29
	1. The Claims' Ordered Combination Implements a Non- Conventional Vehicle-Side Control Architecture.....	30
	2. The Petition Fails at Alice Step Two By Ignoring the Claims' Ordered Combination and Offering No Evidence of Conventionality.	34
V.	GROUND 2: HENDRY FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 1, 6-8, 11, AND 16-18.	38
	A. Hendry Fails to Teach or Suggest a System that “ <i>receive[s] a request to access a user profile stored at a vehicle.</i> ”	39

B.	Hendry Fails to Teach or Suggest a System that “ <i>determine[s], 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.</i> ”	42
C.	Hendry Fails to Teach or Suggest Determining “requested modifications” In Response to an Authorization Determination In Limitation 1[c-3].	44
D.	Hendry Fails to Teach or Suggest a System “ <i>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</i> ” in Claims 6 and 16.....	45
E.	Petitioner Fails to Establish Motivation to Modify Hendry to Arrive at the Claimed Request-Based Profile Authorization Framework.	47
F.	Hendry Fails to Teach or Suggest the Additional Limitations of Dependent Claims 7-8 and 17-18.....	49
VI.	GROUND 3: THE HENDRY-POULSEN COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 3-5 AND 13-15.....	50
A.	Poulsen Fails to Teach or Suggest “Determining Whether Any Conflicts Exist” Between Updated Preferences and Local Preferences.....	51
B.	Petitioner Fails to Establish Motivation to Modify Hendry Based on Poulsen to Add Conflict Detection or Resolution.	53
C.	Poulsen Fails to Teach Dual Verification and Authentication Used to Authorize Access to a User Profile in Claims 6–7 and 16–17.....	57
D.	Petitioner Fails to Establish a Reasonable Expectation of Success for the Asserted Hendry–Poulsen Modifications.	59
VII.	GROUND 4: THE HENDRY–ROVIK COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 9–10 AND 19–20.	61
A.	Hendry-Rovik Fails to Teach or Suggest “ <i>wherein 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.</i> ”	62
B.	Hendry–Rovik Fails to Teach or Suggest “ <i>wherein the template is a global standard template that is common among at least two vehicle manufacturers.</i> ”	64

C.	Petitioner Fails to Establish a Motivation to Modify Hendry Based on Rovik to Implement a Vehicle-Resident Template-Based Profile Architecture.	65
VIII.	GROUND 5: SINGH FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 1, 6–7, 11, AND 16–17.....	68
A.	Singh Fails to Teach or Suggest a System that “ <i>receive[s] a request to access a user profile stored at a vehicle.</i> ”	68
B.	Singh Fails to Teach or Suggest a System that “ <i>determine[s], 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.</i> ”	70
C.	Petitioner Fails to Establish a Motivation to Modify Singh to Add a Request-Based Profile Authorization Framework.	73
D.	Singh Fails to Teach the Additional Limitations of Claims 6–7 and 16–17.	75
IX.	GROUND 6: THE SINGH–CAZANAS–FORSTALL COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 2–8 AND 12–18. 76	
A.	Petitioner Fails to Establish a Motivation to Combine Singh, Cazanias, and Forstall to Arrive at the Claimed Inventions.....	76
B.	The Singh–Cazanias–Forstall Combination Fails to Teach Dual Verification and Authentication Used to Authorize Access to a User Profile In Claims 6–8 and 16–18.....	80
X.	GROUND 7: THE SINGH–ROVIK COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 9–10 AND 19–20.	81
XI.	CONCLUSION.....	82

TABLE OF AUTHORITIES

Cases

<i>Aatrix Software v. Green Shades Software</i> , 882 F.3d at 1128	36
<i>ActiveVideo Networks, Inc. v. Verizon Commc 'ns, Inc.</i> , 694 F.3d 1312 (Fed. Cir. 2012)	56, 57
<i>Alice Corp. v. CLS Bank Int'l</i> , 573 U.S. 208 (2014)	18
<i>Ancora Techs., Inc. v. HTC Am., Inc.</i> , 908 F.3d 1343 (Fed. Cir. 2018)	21, 24, 25, 31
<i>Apotex Inc. v. Wyeth LLC</i> , IPR2014-00115, Paper 94 (Apr. 20, 2015)	54
<i>Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016)	29, 31, 32, 34
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018)	33, 36, 37
<i>CardioNet, LLC v. InfoBionic, Inc.</i> , 955 F.3d 1358 (Fed. Cir. 2020)	26
<i>Data Engine Techs. LLC v. Google LLC</i> , 906 F.3d 999 (Fed. Cir. 2018)	22
<i>DDR Holdings, LLC v. Hotels.com, L.P.</i> , 773 F.3d 1245 (Fed. Cir. 2014)	31, 35
<i>Enfish, LLC v. Microsoft Corp.</i> , 822 F.3d 1327 (Fed. Cir. 2016)	19, 20, 24
<i>Innogenetics, N.V. v. Abbott Lab 'ys</i> , 512 F.3d 1363 (Fed. Cir. 2008)	56, 57

<i>Juniper Networks, Inc. v. Correct Transmission, LLC</i> , IPR2021-00682, Paper 26 (PTAB Oct. 3, 2022)	60
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	55, 57, 78
<i>McRO, Inc. v. Bandai Namco Games Am. Inc.</i> , 837 F.3d 1299 (Fed. Cir. 2016).....	20, 22, 25
<i>Packet Intelligence LLC v. NetScout Sys., Inc.</i> , 965 F.3d 1299 (Fed. Cir. 2020).....	18
<i>SRI Int’l, Inc. v. Cisco Sys., Inc.</i> , 930 F.3d 1295 (Fed. Cir. 2019).....	28
<i>Thales Visionix Inc. v. United States</i> , 850 F.3d 1343 (Fed. Cir. 2017).....	19, 23, 24, 27
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	61
 Statutes	
35 U.S.C. § 101	17, 26

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

The Petition fails because it never grapples with the claim-level security requirements of the '243 patent. The claims do not merely involve vehicle profiles or authentication in the abstract. They require a system that treats user preferences as protected vehicle-resident data, and that enforces security by conditioning modification of that data on a specific, ordered set of vehicle-side control steps.

As claimed, the vehicle must receive a request to access a vehicle-stored user profile; perform verification and/or authentication in response to that request to determine whether access is authorized; and only then permit modification and persistence of vehicle settings in an updated profile. Through this mechanism, the invention prevents unauthorized, unsafe, or inadvertent changes to vehicle settings that directly affect vehicle operation.

None of the cited references—alone or in combination—implements or even contemplates this security architecture. Each addresses a different problem and omits one or more of the steps that give the claimed system its technical effect. Hendry authenticates an external device only to establish a communications link and then automatically reinstates settings. Singh authenticates a driver to unlock and start a vehicle and only afterward loads settings, without receiving or authorizing a request to access profile data. Poulsen is an environment-agnostic framework for saving attributes without vehicle-side access control or conflict resolution. Rovik

generates vehicle-specific settings at a server rather than controlling modification of vehicle-resident profiles. Cazanias and Forstall focus on portability and synchronization for user convenience, not on securing a vehicle-resident profile.

Petitioner's obviousness theories gloss over these requirements, reducing the claims to generic concepts like "profiles," "authentication," or "synchronization," and then reconstructing the invention from unrelated systems. But the technical core of the claims lies in what Petitioner omits: vehicle-enforced authorization of profile modification, performed in response to a request and before any configuration change is allowed to occur. Obviousness cannot be established by removing those constraints and asserting that what remains was known.

The Petition's § 101 challenge fails for the same reason. By stripping away the authorization-based modification at the vehicle and the required control flow, Petitioner recasts a concrete vehicle security system as an abstract idea. Properly understood, the claims are directed to a specific improvement in the security, reliability, and safe operation of vehicle computing systems.

Because the Petition never addresses these requirements, never motivates them, and never shows them to be conventional, every challenged ground fails.

II. THE '243 PATENT

The '243 patent discloses a vehicle-based computing architecture for secure access and management of individualized user profiles that govern 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 system integrates 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. It improves the security and reliability by applying explicit authentication and/or verification gates performed by vehicle-resident hardware and processing, in response to requests to access or modify a vehicle-stored profile. *Id.* at 71:40-58; 87:54-67. The patent also describes optional coordination of profiles across devices, servers, and other vehicles, including conflict determination and reconciliation to preserve consistent vehicle behavior in distributed environments. *Id.* at 88:1-21.

The patent explains that user profiles are stored at the vehicle and include preferences associated with vehicle functions and settings, including operational parameters such as seat position, mirror position, infotainment and navigation settings, HVAC settings, and other vehicle subsystems. *Id.* at 44:23-27; 58:35-47; 62:48-62; 76:35-77:14; Figs. 12A-12D. The vehicle applies these profiles across vehicle sessions so that authorized user settings persist when the same user later accesses the vehicle. *Id.* at 23:26-33; 64:30-50; 74:1-11.

When the vehicle receives 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 (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. *Id.* The disclosed verification and authentication techniques include biometric recognition, device identification, gesture or facial recognition, and cryptographic key exchange executed by the vehicle system. *Id.* at 71:40–58; 72:52–59; 73:24–47; 87:54–68; claims 7–8; Fig. 23 (S2320).

Only after the vehicle determines that the request is authorized does the system determine requested modifications to preferences associated with vehicle functions or settings. *Id.* at 71:59–72:3; 87:63–65; Fig. 23 (S2328). In response to those authorized modifications, the vehicle creates an updated user profile at the vehicle that includes the updated preferences. *Id.* at 73:56–61; 74:17–20; 87:65–67; Fig. 23. The updated profile is stored at the vehicle and governs subsequent vehicle operation, ensuring that authorized configuration changes persist across vehicle sessions. *Id.* at 44:23–27; 57:65–58:20; 59:49–64; 64:30–50; 74:47–55; 75:6–9.

The patent further discloses that, after an updated user profile is created at the vehicle, the vehicle system may 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. Where corresponding profiles already exist at those remote destinations,

the vehicle system performs conflict identification processing to determine whether conflicts exist between updated preferences and previously stored preferences. *Id.* at 88:1–21. When conflicts are detected, the vehicle may overwrite preferences or perform reconciliation to determine which preferences control. *Id.* at 88:4–21.

The patent also explains that user profiles may be structured using templates that define an organized set of preferences. *Id.* at 72:35–49; 72:60–73:23. In some embodiments, the profile is based on a global standard template shared across vehicles or manufacturers, and user modifications to the template are stored as part of the user profile and propagated through profile synchronization. *Id.*

Thus, the '243 patent teaches a vehicle-resident system that receives requests to access a vehicle-stored user profile, determines authorization through vehicle-side verification and/or authentication, determines requested preference modifications only after authorization, and creates and stores an updated user profile at the vehicle reflecting those authorized modifications. *Id.* at 87:44–67.

III. SUMMARY OF THE ASSERTED REFERENCES

Although the asserted references discuss user preferences, device interactions, and vehicle-related functionality in various contexts, they do not disclose or contemplate the security architecture claimed in the '243 patent. Where authentication or identification appear in the prior art, it is performed for purposes unrelated to controlled access to a vehicle-stored user profile—such as establishing

a communications link, identifying a device, or granting physical access to a vehicle—or it is absent altogether. None of the cited systems discloses a vehicle that receives a request to access a user profile as a protected data structure and determines, in response to that request, whether access is authorized before allowing profile data to be accessed or modified. Instead, any application, retrieval, or saving of settings in the prior art occurs automatically, as a consequence of other operations, or through user-driven convenience mechanisms that do not involve vehicle-side authorization of profile access.

By contrast, the '243 patent is directed to a vehicle-resident control architecture that improves the security, integrity, and reliability of vehicle configuration management by requiring the vehicle itself to authorize profile access and modification before any change to vehicle-stored preferences is permitted.

A. Hendry

Hendry describes a system “for establishing user settings of vehicle components” that is “based on a request from an external device to establish a communications link with the communications module of the vehicle.” Ex. 1005, ¶¶ 1, *see also* Abstract, ¶¶ 4, 5, 13, 31.

Hendry’s process begins when the vehicle receives a request from an external device, such as a mobile phone, to establish a communications link with the vehicle’s communications module. *Id.* This request includes identifying information for the

external device, such as a device identifier and a key. *Id.* ¶¶ 17–18, 27, 33. Hendry describes performing verification and/or authentication of the external device in response to this request to determine whether a communications session should be established between the external device and the vehicle. *Id.* Hendry does this by comparing a transmitted key to a stored key, and treating a match as authentication. *Id.* ¶ 19.

If the external device is successfully verified and/or authenticated, Hendry establishes the communications link. *Id.* ¶¶ 18–19. Only after the communications link has been established does Hendry initiate any processes related to user settings. *Id.* At that point, Hendry describes notifying vehicle component modules that a recognized device or user is present and retrieving previously stored settings from local datastores associated with those vehicle components. *Id.* ¶¶ 14 (“Upon receiving notification of the user or the external device 100, each of the modules 104, 112, 116, and 120, will retrieve user settings corresponding to the user or external device 100 from a respective datastore.”), 20, 27 (step 216), 33 (identifying an alternative embodiment in which a central datastore stores component settings). The retrieved settings are then reinstated by the vehicle. *Id.*

Hendry characterizes this approach as “piggybacking.” *Id.* ¶ 19 (“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”). However, Hendry does not describe an actual request received by the vehicle to access a user profile, much less authentication or verification of such a request. Instead, Hendry authenticates only the general request to establish a communications link and then, based on the device identifier, automatically retrieves and applies previously stored user settings.

Hendry’s authentication and verification processes are thus performed at the communications layer and are used to control whether a communications link is established between the external device and the vehicle. Hendry does not describe receiving, authenticating, or authorizing *a request to access a user profile* stored at the vehicle. Nor does Hendry describe performing authentication or verification in response to a request to access or modify a user profile. Instead, once a communications link is established, Hendry automatically retrieves and reinstates saved settings. Ex. 2022 ¶¶ 57-64.

B. Poulsen

Poulsen describes a generalized profile-management framework for storing, retrieving, and applying collections of attributes—referred to as “profiles”—to selected content across a wide range of computing environments. Ex. 1006 ¶¶ 2–3. Poulsen is not directed to vehicle systems or vehicle-specific user profiles, but instead addresses profile portability and reuse in broadly applicable software and computing contexts. *Id.* at Abstract, (“Disclosed are methods for creating, applying,

using and retrieving ... profiles [that] can be shared in various environments and across various applications” such as in CAD software), ¶¶ 3–6.

A central concept of Poulsen is the decoupling of profiles from content, such that profiles may be stored independently in profile repositories and later retrieved and applied to content using links, identifiers, or pointers. *E.g.*, Ex. 1006 ¶¶ 3, 6, 35–38, Fig. 1. Poulsen explains that a profile may include a plurality of attributes corresponding to configuration parameters, display settings, application states, or other environment-specific characteristics. *E.g., id.* ¶¶ 35, 37, 52, 61.

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. *E.g.*, Ex. 1006 ¶¶ 4, 51, 68, 78, Figs. 3, 9, 12. Poulsen further allows users to apply entire profiles or only selected subsets of attributes, and to create temporary or derived profiles based on selected attributes. *Id.*

Poulsen supports storing profiles in a variety of locations, including internal storage, external files, databases, removable media, and network-accessible repositories. Ex. 1006 ¶¶ 42, 49, 105–117, Figs. 22–23. Profiles may be accessed locally or remotely, and Poulsen describes dynamically linking profiles such that changes to one profile may propagate to other linked profiles. *Id., see also id.* ¶ 43. Poulsen also discloses user interfaces that allow users to define, store, recall,

overwrite, delete, and otherwise manage multiple profiles and sets of profiles, including default profiles that may be automatically applied when content is loaded. Ex. 1006 ¶¶ 45–47, 49–50, 86. While Poulsen allows a user to overwrite the entire profile or selectively save preferences, it does not describe or address conflict detection and subsequent resolution. Instead, Poulsen’s profile-management framework relies on user-driven actions—such as selecting profiles, choosing subsets of attributes, or confirming overwrites—without any automated determination of whether preferences conflict across multiple stored profile instances. *Id.*

In addition, Poulsen’s disclosure is environment-agnostic. Poulsen references that its techniques can be applied in many different contexts, and vehicles are merely one of numerous potential environments Poulsen identifies and are not treated with any particular technical specificity. For example, Poulsen does not describe vehicle-side authorization of requests to access user profiles, and does not address security or safety concerns unique to vehicle operation. Ex. 2022 ¶¶ 74-77.

C. Rovik

Rovik is directed to “apparatuses and methods for adjusting a position of at least one component of a vehicle.” Ex. 1007, Abstract. Rovik explains that user-adjustable vehicle components—such as seats and mirrors—are typically configured only for a particular vehicle, and that when a user enters a “different make or model

from the user's usual vehicle," the user must spend additional time searching for preferred settings. *Id.* at 1:22–29. To address this inconvenience, Rovik proposes storing vehicle-specific user settings at a remote server for transmission to other vehicles. *Id.* at 1:30–32.

Rovik also describes a server-side process in which a "standardized" user profile is used in combination with a vehicle-specific profile to generate new user settings for vehicles the user has not previously driven. *Id.* at Figs. 5–6, 9; 2:6–23; 8:66–10:25; 12:50–13:13. Rovik describes this standardization as occurring solely at the server, where user preferences are normalized "so as to apply to a standard vehicle." *Id.* at 9:37–42. The "standard vehicle" is an internal reference used to account for geometric differences between vehicle models, such as seat-track distances. *Id.* at 13:2–6; *see also* 8:7–10, 8:32–39, 8:55–59.

Consistent with this architecture, Rovik does not transmit this standardized user profile to vehicles. Instead, the standardized profiles simply serve as a tool for generating new settings that account for differences in the interior geometries and capabilities of a particular vehicle. *Id.* at Fig. 9 (steps 720–722); 8:66–10:25; 12:50–13; *see also id.* at 8:32–39; 8:55–59. After performing this process, Rovik transmits only the generated vehicle-specific settings to the vehicle. *Id.* at Fig. 9 (step 722); 2:6–23; 13:10–13; Ex. 2022 ¶¶ 78–83.

D. Singh

Singh describes an “intelligent vehicle” designed to allow multiple drivers to operate a single vehicle by authenticating each driver before granting access to the vehicle itself. Ex. 1008 at Abstract; ¶¶ 2, 4, 38–39. Singh explains that this approach addresses concerns related to vehicle security and the use of a shared vehicle by multiple drivers, while also allowing different drivers’ preferences to be applied once the driver has been granted access to the vehicle. *Id.* ¶ 2.

To that end, Singh describes a vehicle entry architecture in which the driver’s door is equipped with a password console and a fingerprint scanning console, the latter being locked behind a metallic shutter. *Id.* ¶ 4. These components are used to authenticate the driver before allowing entry into the vehicle. *Id.* ¶¶ 36–40. The driver must first enter a password, which the controller compares against entries in the vehicle database. *Id.* ¶ 38. If the password matches, the system opens the shutter covering the fingerprint scanner and prompts the driver to provide a fingerprint impression. *Id.* ¶¶ 4, 22, 38. The fingerprint scanner then captures the fingerprint and compares it against stored entries associated with the entered password to verify the identity of the driver. *Id.* ¶¶ 23, 39.

Singh explains that this process is a stepwise vehicle-entry sequence. If the password does not match, the fingerprint scanner remains inaccessible, and the process returns to password entry. *Id.* ¶ 38; Fig. 3. If the fingerprint does not match,

the system does not proceed further. *Id.* ¶¶ 39–40; Fig. 3 (explaining that “car is locked after two tries”). Only after both steps are successfully completed does the system unlock the vehicle door and permit the driver to open the door. *Id.* ¶¶ 23, 40; Fig. 3. After the door is opened, Singh explains that the controller then sends a signal to start the vehicle’s engine. *Id.* ¶ 40 (“The third step in the current invention is initiated only when the result from the second step is positive”); Fig. 3.

Singh explains that access to stored driver preferences occurs only after the vehicle has been unlocked and started, stating that “[o]nce the verification has been performed and the vehicle started, the Controller Unit of the current invention loads the essential vehicle features for the driver.” *Id.* ¶ 41; Fig. 3. Those settings are stored in user profiles maintained in an operator database and include files containing seat settings, mirror positions, climate preferences, and other vehicle features. *Id.* ¶ 33. Thus, Singh’s authentication and verification processes are directed to determining whether a driver is permitted to enter and operate the vehicle, rather than to authorizing access to a user profile in response to a request.

After the security measures have been completed, the driver has entered the vehicle, the engine has started, and the driver’s preferences have been loaded, Singh allows the driver to modify stored preference files through a graphical user interface. *Id.* ¶ 62, Fig. 3. Singh explains that the controller records any changes made by the driver and saves those changes when the driver completes the task or turns the

vehicle off. *Id.* at Fig. 3. Singh does not describe the vehicle receiving a request to access a user profile, nor does it describe any security mechanism that evaluates or authorizes access to profile data based on such a request.

Accordingly, Singh discloses a system in which password and fingerprint checks are used exclusively to control vehicle access and operation. Only after those checks are completed does Singh load or permit modification of driver-specific settings. Singh does not disclose any separate authorization decision governing access to user profile data once vehicle entry has been granted. Ex. 2022 ¶¶ 65-73.

E. Cazan

Cazan is directed to a system for portability of vehicle preference settings across different vehicles, particularly vehicles that a user does not typically operate, such as rental cars or borrowed vehicles. Ex. 1009 at 1:15–40. The reference focuses on user convenience in restoring preferred vehicle configurations when transitioning between vehicles. *Id.*

Specifically, Cazan describes a “driver profile” as a collection of user preference settings for configurable vehicle components, such as seat position, mirror positions, radio presets, HVAC settings, and navigation display preferences. *Id.* at 1:5–11, 49–67. These settings are treated as comfort and convenience parameters, and Cazan frames the problem it addresses as the inconvenience associated with manually re-adjusting such settings when entering a different

vehicle. *Id.* at 1:15–40. The solution proposed by Cazanias is to store these preference settings on a remote server and download them to another vehicle, optionally applying transcoding when the vehicles are of different types. *Id.* at 1:44–54, 15:33–45, 16:9–30.

Cazanias does not discuss the use of security measures in connection with profiles that are transmitted to and from the remote server, or otherwise describe authentication or verification processes governing profile access or modification. Cazanias assumes that possession of an identifier—such as a key fob ID or mobile directory number—is sufficient to associate a set of preference settings with a user. *Id.* at 12:12–13:30. Once identified, the system retrieves or updates the corresponding preference profile without describing any additional authorization assessment beyond an identifier. Ex. 2022 ¶¶ 84–85.

F. Forstall

Forstall is directed to systems and methods for synchronizing information between a mobile device and a vehicle device, particularly in connection with location and navigation functionality. Ex. 1010 at Abstract, ¶¶ 3–9. In general, Forstall describes receiving location information stored in vehicle memory device at a mobile device and updating the mobile device based on that information when the mobile device is proximate to the vehicle. *Id.* ¶ 6 (“The method includes 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.”), 74-76. Forstall also describes transmitting location information stored on a mobile device to a vehicle device and updating the vehicle device based on that information under similar proximity conditions. *Id.* ¶¶ 7-8.

The disclosed systems use positioning technologies such as GPS receivers, wireless networks, and onboard sensors including accelerometers, compasses, and gyroscopes to determine, estimate, or track device location, including through dead-reckoning techniques when GPS is unavailable. *Id.* ¶¶ 5, 36, 45, 67-69, 72-74.

Forstall further describes synchronization mechanisms that allow information stored on one device to be provided to the other device. *Id.* ¶¶ 82-83, 92, 97-99, Figs. 5, 6. For example, Forstall discloses an “auto-update device or vehicle with new information” option that, when enabled, automatically provides newly stored information on one device to the other device. *Id.* ¶ 90. Forstall also describes a conflict-resolution button that a user can select to which that dictates which device’s information is copied onto the other device during synchronization. *Id.*

Forstall does not describe user profiles, nor does it address systems for controlling access to, authenticating requests for, or authorizing modification of user-specific profile data stored on a vehicle or server. *See id.* ¶ 97-99. Instead, Forstall is directed to functional data synchronization between a mobile device and

a vehicle device, primarily to support navigation, location tracking, and related convenience features. Ex. 2022 ¶¶ 86-88.

IV. GROUND 1: THE CHALLENGED CLAIMS ARE PATENT ELIGIBLE UNDER 35 U.S.C. § 101.

The Petition’s § 101 challenge rests on the familiar but flawed move of stripping the challenged claims of their technological context and recasting them as nothing more than profile management or updating information. That characterization bears little resemblance to what the claims actually require.

The claims are directed to a vehicle-side computing architecture that addresses technical problems unique to computer-controlled vehicles—securely controlling access to safety-relevant settings, preventing unsafe or inconsistent configuration changes (especially during operation), and maintaining system integrity as profiles move across vehicles, devices, and servers. These problems do not arise in ordinary data-processing systems because vehicle settings directly control how the vehicle operates, and unauthorized or conflicting changes can compromise reliability and passenger safety.

When evaluated as a whole, the claims improve the operation, security, and reliability of vehicle computing systems by preventing unauthorized configuration changes, avoiding inconsistent system states across devices and vehicles, and protecting vehicle functionality during operation.

Petitioner’s contrary framing depends on ignoring those requirements. By abstracting away the vehicle, the authorization gates, the locus of control, and the reconciliation logic, the Petition reduces the claims to a result untethered from the means by which the invention achieves it. Section 101 does not permit that approach. Properly characterized, the challenged claims are not directed to an abstract idea at all—and even if the Board reaches Alice Step Two, the Petition still fails to show the claimed combination is routine or conventional.

A. Alice Step One: The Claims Are Directed to a Vehicle-Side Computing Architecture That Improves the Operation and Security of Vehicle Computing Systems.

At Alice Step One, the question is what the claims are directed to as a whole, in light of the specification—not whether they can be recast at a high level of abstraction as involving “profiles” or “information.” *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208 (2014); *Packet Intelligence LLC v. NetScout Sys., Inc.*, 965 F.3d 1299, 1309 (Fed. Cir. 2020). When read that way, the challenged claims are directed to a vehicle-side computing architecture that governs when and how vehicle settings may be accessed, modified, and reconciled by requiring authorization and enforcement at the vehicle itself. Claims 1–20; Ex. 2022 ¶¶ 90–92, 106–111, 136–147.

That framing matters because claims are not abstract at Step One when they are directed to a specific improvement in the operation, security, or reliability of a computing system—rather than an abstract result implemented on generic hardware.

Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1335–36 (Fed. Cir. 2016). The inquiry turns on what the claims require the system to do and how they require it to do it, not on whether they involve information processing.

That principle applies with particular force where, as here, the claims concern a computer-controlled physical system. Ex. 2022 ¶¶ 136–138, 146–147. Vehicle settings directly control how a vehicle operates, and unauthorized or inadvertent configuration changes compromise both system reliability and passenger safety. Claims that impose architectural constraints on where control resides and when system state may change are directed to a technological solution—not an abstract idea. *See Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1348–49 (Fed. Cir. 2017) (finding claims patent eligible where they recited a specific configuration for improving the operation of a tracking system).

The challenged claims fit squarely within that line of authority. As explained below, they define a vehicle-side control architecture that allocates authorization and enforcement to the vehicle, requires a specific sequence of operations before any vehicle setting may be changed, and constrains how vehicle-created profile updates are propagated and reconciled across distributed systems. That is what the claims are directed to—and it is why they are not abstract at Alice Step One.

1. The Claims Define a Vehicle-Side Control Architecture Governing Access to and Modification of Vehicle Settings.

The challenged claims are not directed to generic data manipulation. As in *Enfish*, they define a particular system organization in which data is stored and used in a way that directly controls system operation, rather than merely reciting the manipulation of information in the abstract. 822 F.3d at 1335–37.

The claims begin with a user profile stored at the vehicle—not at a remote server or in the cloud. Claims 1, 11. That profile includes preferences “associated with functions or settings of the vehicle.” *Id.* As the specification explains, those preferences are not abstract labels or informational metadata. They are operational parameters that directly affect how the vehicle functions, including seat position, mirror position, HVAC settings, infotainment settings, and access and parental control restrictions. *E.g.*, Ex. 1001 at 64:39-50; 66:25-33; 67:15-31; 76:35-77:15; 85:4-29; 85:67-86:4; 90:13-26.

Claims directed to system-level control over how a computer-driven machine operates are not abstract at Alice Step One, because they focus on improving system operation itself, not on manipulating information for its own sake. *See Enfish*, 822 F.3d at 1335–36 (claims patent eligible where they focused on a specific system architecture that improved computer functionality); *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1314–16 (Fed. Cir. 2016) (finding claims not abstract where they recited specific rules that constrained how the system operated).

Access to vehicle settings is not automatically granted. The claims require that, in response to a request to access the vehicle-stored profile, the vehicle performs verification and/or authentication to determine whether the request is authorized. Claims 1, 11. The specification emphasizes that this authorization is performed by the vehicle control system itself, using technical security mechanisms such as biometric recognition, device identification, gesture or facial recognition, and cryptographic key exchange. *See* Ex. 1001 at FIG. 23; 71:40-58; 72:50-59; 73:24-47; 81:33-42; 87:54-67. Petitioner’s expert agreed that verification and authentication are important technical security measures for preventing unauthorized access to user profiles. Ex. 2023 at 30, 33.

Placing authorization and enforcement logic at a specific system component to solve a security problem is a concrete architectural choice, not an abstract idea. *See* Ex. 2022 ¶¶ 102–105, 120–123; *see also Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1348–49 (Fed. Cir. 2018) (finding claims patent eligible where security verification was anchored to a particular device component).

Only after the vehicle determines that a request is authorized may any modification occur, and the claims then require creating an updated user profile at the vehicle based on those authorized modifications. Claims 1, 11. Even in a distributed environment—where profiles may later be transmitted to mobile devices,

cloud servers, or other vehicles—the vehicle remains the authoritative source of configuration state. Ex. 2022 ¶¶ 99–105, 110–111, 118–119, 125–130, 146–147.

That ordered sequence is central to the invention. The claimed system must:

- (1) receive a request to access a vehicle-stored user profile;
- (2) determine authorization of the request through vehicle-side verification and/or authentication;
- (3) determine requested modifications only after authorization of the request; and
- (4) create an updated user profile at the vehicle based on those authorized modifications.

See Claims 1, 11.

This is not a result-oriented description of “updating information.” Ex. 2022 ¶¶ 109–112, 141–143. It is a claimed control flow that governs *when* and *how* vehicle settings may change. Claims that impose specific sequencing or rules to constrain system behavior—like the ones at issue here—are not abstract where that sequencing improves system operation. *See McRO*, 837 F.3d at 1313–16; *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1008–09 (Fed. Cir. 2018).

The specification explains why this sequencing matters in the vehicle context. Vehicle settings directly affect safety-relevant and operational systems, and unauthorized or inadvertent changes—particularly while a vehicle is in use—can

compromise reliability and passenger safety. *E.g.*, Ex. 1001 at FIGS. 14, 28; 67:26-31; 81:33-42; 82:33-57; 83:7-12; 85:60-86:4; 90:14-26. Petitioner’s expert agreed that settings such as mirrors, seats, and steering wheel orientation directly affect vehicle safety and should not be changed without authorization, especially during operation. Ex. 2023 at 22, 49–50.

By requiring authorization first, modification second, and enforcement at the vehicle, the claims reflect a deliberate architectural solution to technical problems in computer-controlled vehicles—not a result-oriented abstraction. The Federal Circuit has repeatedly recognized that claims directed to specific system architectures designed to improve safety, reliability, or control in real-world systems are patent eligible. *E.g.*, *Thales*, 850 F.3d at 1348–49 (claims patent eligible where they recited a specific system architecture that improved operation of a real-world tracking system).

Taken as a whole, the claims improve the operation, reliability, and safety of vehicle computing systems themselves by reallocating control, authorization, and enforcement to the vehicle, imposing an authorization-first sequencing before configuration changes, and constraining how system state may change and propagate. Ex. 2022 ¶¶ 93–104, 118–119, 136–147, 177–178. That is precisely the kind of architectural improvement the Federal Circuit has found patent eligible at

Alice Step One. *See Enfish*, 822 F.3d at 1335–36; *Thales*, 850 F.3d at 1348–49; *Ancora*, 908 F.3d at 1347–49.

The dependent claims reinforce the vehicle-side control architecture the claims are directed to by specifying how authorization, control, and synchronization are implemented at the vehicle.

Several dependent claims require particular vehicle-side verification and authentication mechanisms before any vehicle-stored profile may be accessed or modified. Claims 6–8, 16–18. Those mechanisms include biometric recognition, gesture or facial recognition, device identification, and cryptographic key exchange between the vehicle and a mobile device. *Id.*; Ex. 2022 ¶¶ 112–113, 123, 140, 154–155. In a vehicle context, these are not generic design choices. While Petitioner’s expert considered such techniques to be known in software systems generally, he was unable to characterize them as a usual or standard feature in passenger vehicles at the time of the invention. Ex. 2023 at 56–59, 65–66.

Other dependent claims address what happens after an authorized modification is made at the vehicle. Claims 2–5 and 12–15 require controlled propagation of the vehicle-created profile to mobile devices, cloud servers, remote servers, or other vehicles—together with conflict detection and reconciliation logic where a local profile already exists. *See* Ex. 2022 ¶¶ 114–116, 128–130, 144–146. In a vehicle environment—where settings govern seats, mirrors, HVAC systems,

access restrictions, and parental controls—this logic solves a technical problem that does not arise in ordinary data-processing systems: preventing inconsistent or unsafe vehicle configurations across distributed devices and vehicles. *See* Ex. 1001 at 66:34-40; 67:15-31; 71:59-63; 74:9-20; 82:40-46; 85:63-86:4; 88:4-21; 90:13-26; Ex. 2022 ¶¶ 97–104, 116, 130, 164.

Still other dependent claims require that user profiles be created and updated relative to templates, including optional global standard templates shared across vehicle manufacturers. Claims 9–10, 19–20. As the specification explains, these templates promote interoperability and consistency in how vehicle settings are structured and enforced across different vehicles and systems. *E.g.*, Ex. 1001 at 71:59-63; 72:35-74:9; Ex. 2022 ¶¶ 117, 131–133, 145, 165. These limitations further confirm that the invention concerns structured vehicle configuration control, not free-form information editing or generic profile management.

As the Federal Circuit has made clear, dependent claims that further specify how a claimed system architecture is implemented do not introduce abstract ideas at Alice Step One. They reinforce what the claims are directed to as a whole. *See McRO*, 837 F.3d at 1314–15 (claims not abstract where limitations specified the rules and structure governing system behavior); *Ancora*, 908 F.3d at 1348–49 (security-focused limitations anchored to a particular system component reinforced patent-eligible architecture).

Properly understood, the challenged claims—independent and dependent alike—are directed to a concrete vehicle computing solution that governs access to and modification of vehicle settings through vehicle-side authorization, enforcement, and controlled synchronization.

2. The Petition’s Step-One Framing Improperly Abstracts Away the Claimed Vehicle-Side Control Architecture.

The Petition does not engage with the vehicle-side control architecture the claims actually recite. Instead, it replaces the claims the Board must evaluate with a stripped-down abstraction, characterizing the invention as nothing more than “receiving,” “determining,” “updating,” and “transmitting” information. Pet. at 20–23; Ex. 1003 ¶¶ 132–135, 137–139. Courts have repeatedly rejected this kind of verb-stripping analysis, which asks whether generic functions exist in the abstract rather than whether the claims recite a specific technological solution. *See CardioNet, LLC v. InfoBionic, Inc.*, 955 F.3d 1358, 1371 (Fed. Cir. 2020) (rejecting characterization of claims as merely “collecting, analyzing, and reporting data” where it ignored the claims’ specific technical requirements).

The same abstraction appears in the Petition’s element-by-element analysis, which reduces the claims to generic verbs and declares them abstract. Pet. at 21–22; Ex. 1003 ¶¶ 133–135, 140–148. By fragmenting the claims and ignoring where actions occur and under what constraints, the Petition ensures an abstract

characterization before the analysis begins—contrary to Alice Step One, which asks whether the claims as a whole are directed to a technological solution.

The Petition’s abstraction is achieved only by striking from the claims the very limitations that define how the system operates—including the vehicle-stored profile, vehicle-side authorization, authorization-first sequencing, vehicle-created profile updates, and constrained synchronization and reconciliation across distributed systems. *See* Ex. 2022 ¶¶ 148–156. Section 101 does not permit that approach. Where claims specify how a system is architected and where control resides, they are directed to a concrete technological solution, not an abstract idea. *See Thales*, 850 F.3d at 1348–49 (finding claims patent eligible where they recited a specific system architecture for improving the operation of a tracking system).

The Petition’s table-based treatment of claim 1 illustrates the error. The Petition reduces the claim to four generic verbs—then asserts that such steps are “always” abstract. Pet. at 21–22. But Alice Step One does not ask whether generic verbs exist in isolation. It asks what the claims require the system to do, how they require it to do it, and why that matters. By ignoring the vehicle-side authorization gate, the sequencing of operations, and the location of control, the Petition substitutes a conclusion for an analysis.

The Petition attempts to justify its abstraction by asserting that the claims could be performed “mentally” or with “pen and paper.” Pet. at 24–25; Ex. 1003 ¶¶

137–139. That argument fails because it assumes away the computerized vehicle environment the claims require, including system-enforced authorization and control over safety-relevant vehicle operations.

Claim 1, for example, requires vehicle-side verification or authentication before access to or modification of a vehicle-stored profile is permitted. Those are system-enforced security operations that cannot be performed mentally. At deposition, Petitioner’s expert did not identify any meaningful way in which the claimed vehicle-side authorization and profile control could be implemented without a computerized system enforcing access and modification. Ex. 2023 at 37–39. Courts have rejected this maneuver. *See SRI Int’l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1304 (Fed. Cir. 2019) (finding the human mind not equipped to perform the claimed network-security functions).

The same flaw carries through the Petition’s treatment of the dependent claims, which are dismissed as “trivial” or “conventional” without analysis. Pet. at 25–27; Ex. 1003 ¶¶ 140–148. At Alice Step One, however, dependent claims matter because they reinforce what the claims are directed to as a whole. Here, they further specify how the vehicle-side control architecture is implemented, including vehicle-based authorization, controlled profile propagation, conflict detection and reconciliation, and structured profile templates—limitations that define a concrete technological solution, not an abstract idea.

When the claims are evaluated as a whole, and in light of the specification, they are directed to a concrete vehicle computing architecture for governing access to and modification of vehicle settings under authorized, constrained conditions—not to an abstract idea. That framing governs the remainder of the § 101 analysis.

B. Even If the Board Were to Proceed to Alice Step Two, the Claims Recite an Inventive Vehicle-Side Control Architecture That Was Neither Routine nor Conventional.

Even if the Board were to proceed to Alice Step Two, the challenged claims remain patent eligible because they recite an inventive concept—an ordered combination of elements that implements a concrete, vehicle-specific control architecture.

The inventive concept does not reside in any single claim limitation viewed in isolation. It lies in the architecture as a whole: allocating authorization and enforcement to the vehicle itself; requiring authorization before any modification of vehicle settings; making the vehicle the authoritative source of updated configuration state; and constraining how vehicle-created profiles propagate and are reconciled across devices and vehicles in a distributed environment. Ex. 2022 ¶¶ 157–163, 167–168. That kind of system-level design is exactly what the Federal Circuit has recognized as an inventive concept under Step Two. *See Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016)

(inventive concept may arise from the ordered combination of claim limitations, even if individual components were known).

Critically, Step Two does not ask whether individual elements—such as verification, authentication, profile storage, or data transmission—were known in isolation. It asks whether the claimed combination, arranged as the claims require and implemented in the claimed technological context, was “well-understood, routine, and conventional.” *See id.* at 1350. Where, as here, the claims specify a non-conventional allocation of control, sequencing, and enforcement tailored to the operation of computer-controlled vehicles, they recite an inventive concept.

As explained below, the Petition never engages with that ordered combination. It disassembles the claims into generic components, labels them “conventional,” and stops there. That is not enough under Alice Step Two.

1. The Claims’ Ordered Combination Implements a Non-Conventional Vehicle-Side Control Architecture.

The challenged claims recite an inventive concept because, viewed as an ordered combination, they implement a non-conventional vehicle-side control architecture for governing access to and modification of vehicle settings.

At the core of that architecture is a deliberate allocation of control to the vehicle itself. The claims require that a user profile governing vehicle operation is stored at the vehicle and may be accessed or modified only after the vehicle performs verification and/or authentication in response to an access request. Claims 1, 11; *see*

also Claims 6–8, 16–18. As the specification explains, the preferences stored in that profile directly control how the vehicle operates, including seating, mirrors, HVAC, infotainment, parental controls, and access restrictions. *E.g.*, Ex. 1001 at 67:15-31; 71:40-72:34; 73:24-47; 85:42-86:4; 90:13-26.

Because those settings affect the vehicle’s physical operation, the claims require that authorization be established at the vehicle before any modification is permitted. *E.g.*, Claim 1; Ex. 2022 ¶¶ 157–163, 166–168, 179. Claims that recite a specific security or access-control architecture—rather than merely invoking security in the abstract—can supply an inventive concept at Alice Step Two. *See Ancora*, 908 F.3d at 1348–49; *see also Bascom*, 827 F.3d at 1350-51.

That authorization-first sequencing—verification or authentication first, modification second, enforcement at the vehicle—is central to the invention’s technical solution. The specification repeatedly emphasizes that vehicle control systems must prevent unauthorized or inadvertent configuration changes that could compromise safety or reliability while the vehicle is in use. *E.g.*, Ex. 1001 at 71:40-72:34; 73:24-39; 81:33-42; 82:33-83:12; 85:43-53; 85:67-86:4; 92:59-65. By placing verification, authentication, and enforcement logic at the vehicle, the claims adopt a specific architectural design tailored to computer-controlled vehicles, not a generic data-management scheme. *See DDR Holdings, LLC v. Hotels.com, L.P.*, 773

F.3d 1245, 1257–59 (Fed. Cir. 2014) (finding claims reciting a specific system architecture that altered conventional operation supplied an inventive concept).

The claims further require that, once authorization is established, the updated profile is created at the vehicle and governs how the vehicle will operate going forward. Claims 1, 11. The specification makes clear that the vehicle control system is the authoritative source of configuration state: profiles are “created,” “stored,” and “enforced” by the vehicle itself to control vehicle behavior. *E.g.*, Ex. 1001 at 65:67-66:53; 67:15-31; 74:11-34; 85:67-86:4. This is not a conventional client-server model in which a remote system passively updates data that the vehicle later consumes. The vehicle is the locus of control. Where claims recite a non-conventional allocation of functionality within a system, they are not merely applying routine computer functions. *See Bascom*, 827 F.3d at 1350.

The dependent claims further reinforce that non-conventional architecture by specifying how it is implemented. Claims 2–5 and 12–15 require controlled propagation of vehicle-created profiles to other devices and vehicles, together with conflict detection and reconciliation logic. Claims 9–10 and 19–20 require template-based profile structures, including global standard templates. Those limitations matter at Step Two not because they add features in the abstract, but because they underscore that the claimed system reflects a coordinated architectural design governing where control resides, when changes are permitted, and how

configuration state propagates across distributed components. Ex. 2022 ¶¶ 159–166, 169–176, 180.

The Petition never supplies evidence that this kind of vehicle-side enforcement and reconciliation architecture was routine or conventional in passenger vehicles. *Id.* ¶¶ 169–176. Petitioner’s expert did not either. *Id.* He testified that he had not analyzed conventional use in passenger vehicles and used “conventional” only to mean known in software systems generally. *Id.* at 60, 70–71. That is not enough under Alice Step Two. Whether a claimed combination was “well-understood, routine, and conventional” is a factual question that requires evidence. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368–69 (Fed. Cir. 2018).

Viewed as an ordered combination, the claims improve the operation of vehicle computing systems themselves. They prevent unauthorized access to vehicle settings, avoid conflicting configuration states across distributed systems, and ensure that safety-relevant vehicle behavior is governed by profiles created under vehicle-side control. Those improvements address problems unique to computer-controlled vehicles—not generic information processing. *E.g.*, 1001 at 67:7-31; 71:40-73:47; 85:43-86:4; 88:1-21; 92:59-65; Ex. 2022 ¶¶ 177–180. Improvements to the operation, security, and reliability of a computer-based system itself constitute an inventive concept at Alice Step Two.

2. The Petition Fails at Alice Step Two By Ignoring the Claims’ Ordered Combination and Offering No Evidence of Conventionality.

At Alice Step Two, the burden rests squarely on Petitioner to show that the challenged claims recite nothing more than activity that was “well-understood, routine, and conventional” at the time of the invention. The Petition does not come close to carrying that burden.

Rather than analyzing the claims as an ordered combination, the Petition disassembles them into isolated elements, labels those elements “generic,” and then declares the inquiry over. That is not the law, and it is not a substitute for evidence. Alice Step Two turns on whether the claimed combination, arranged as the claims require and implemented in the claimed technological context, reflects a conventional implementation—not whether individual components were known in isolation. *See Bascom*, 827 F.3d at 1350.

The Petition’s Step Two analysis simply repeats its Step One error. After abstracting the claims to “receiving,” “determining,” “updating,” and “transmitting” information, the Petition asserts—without analysis—that those same steps are “routine” and “conventional.” Pet. at 27–29. But Step Two does not ask whether generic verbs were known in the abstract. It asks whether the vehicle-side control architecture the claims actually recite was conventional. The Petition never addresses that question, which alone is fatal under *Bascom*.

Most notably, the Petition never grapples with the claims’ core architectural requirements:

- (1) vehicle-side authorization before profile access or modification;
- (2) vehicle-side creation of updated profiles that govern vehicle operation;
and
- (3) constrained synchronization of vehicle-created profiles across devices
and vehicles through conflict detection and reconciliation logic.

See Claims 1–5, 11–15.

Instead, those requirements are treated as interchangeable “data processing” steps, untethered from the system architecture the claims impose to protect vehicle operation. Pet. at 20–23, 27–29. Where, as here, claims specify a particular allocation of control and sequencing to solve a technology-rooted problem, that architecture cannot be dismissed as conventional without evidence. *See DDR Holdings*, 773 F.3d at 1257–59.

That omission is dispositive. The specification does not describe a conventional profile system repurposed for vehicles. It describes a vehicle control architecture designed to prevent unauthorized or unsafe configuration changes to systems that directly affect how the vehicle physically operates. *E.g.*, Ex. 1001 at 82:33-46; 83:7-34; 85:43-86:4; Ex. 2022 ¶¶ 96–100, 127–130. The Petition identifies no prior art system—vehicle-based or otherwise—that implemented this

vehicle-side allocation of control, authorization-first sequencing, and constrained synchronization across vehicles, devices, and servers.

Petitioner’s expert testimony underscores that evidentiary gap. Mr. Denning testified that he has limited experience with passenger vehicle systems and did not analyze whether vehicles at the time of the invention implemented the claimed architecture. Ex. 2023 at 59–60, 166. His use of “conventional” referred only to software concepts generally, not to vehicle computing systems in particular. *Id.* at 60, 70–71. That is insufficient under Alice Step Two.

The expert declaration fares no better. It asserts, in conclusory fashion, that the claims recite “generic computer functions” and “routine data management.” Ex. 1003 ¶¶ 132–135, 140–145. But those assertions are untethered from the claim language and the specification. The declaration does not analyze the claims as an ordered combination, does not explain why vehicle-side authorization before modification was conventional in vehicle computing systems, and does not identify any evidence showing that conflict detection and reconciliation of vehicle profiles across distributed vehicles and devices was routine at the time of the invention. Conclusory statements of that sort cannot establish conventionality at Step Two. *See Berkheimer*, 881 F.3d at 1368; *see also Aatrix*, 882 F.3d at 1128.

The Petition’s treatment of the dependent claims highlights the same flaw. Claims 2–10 and 12–20 are dismissed as adding only “trivial” or “conventional”

details, without any attempt to explain why biometric verification, cryptographic authentication, template-based profiles, global standard templates, conflict detection, or reconciliation were routine in vehicle computing systems. Pet. at 25–27; Ex. 1003 ¶¶ 140–148. Labeling technical features “well-known” does not make them so—particularly where the specification explains their role in preserving vehicle safety, security, and configuration consistency. *See Berkheimer*, 881 F.3d at 1368–69.

Nor does the Petition identify any evidence—industry standards, contemporaneous vehicle systems, textbooks, or prior art vehicles—showing that the claimed vehicle-side control architecture was conventional. There is no showing that vehicles routinely allowed profile modifications without vehicle-side authorization, or that they conventionally reconciled conflicting vehicle profiles across vehicles, mobile devices, and cloud systems. Absent such evidence, Petitioner cannot carry its Step Two burden.

Petitioner ultimately asks the Board to accept a Step Two conclusion without a Step Two analysis. Section 101 requires more. Because the Petition and its expert fail to show that the claims’ ordered combination reflects activity that was well-understood, routine, and conventional, Ground 1 fails at Alice Step Two as well.

V. GROUND 2: HENDRY FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 1, 6-8, 11, AND 16-18.

Petitioner fails to prove its obviousness arguments in Ground 2, which challenge claims 1, 6-8, 11, and 16-18. The claims of the '243 patent are concerned with securing user profiles, including controlling whether and how those profiles may be accessed and modified. To that end, the claims require that a request to access a user profile be subjected to one or more verification and/or authentication processes, and that authorization to access or modify profile data be determined based on the outcome of those processes. As Dr. Martin explains, the steps of claims 1 and 11 are conditionally linked and performed in a required order: authorization is determined in response to the request to access the profile and requested modifications and profile updates occur only in response to a favorable authorization determination. Ex. 2022 ¶ 183. This architecture provides enhanced security by preventing inadvertent, unauthorized, or unintended changes to user-specific vehicle preferences. Ex. 2022 ¶¶ 43. 178.

Hendry, by contrast, is directed to allowing mobile devices to connect to the vehicle communication module, and to then reinstate previously saved vehicle settings. Ex. 1005 ¶¶ 1, 4-5, 13, 17-18, 27; Ex. 2022 ¶¶ 186, 188-190, 214. Verification or authentication in Hendry occurs only at the communications layer and serves only to determine whether a communications session should be

established. *Id.* Hendry does not receive, authenticate, or authorize a request to access a user profile. *Id.*

Because Hendry authenticates connectivity rather than profile access, and automatically reinstates stored settings rather than securing profile access or modification, it lacks the profile-level security framework required by the challenged claims. *Id.* As explained below, Petitioner fails to acknowledge these substantive architectural distinctions, and never identifies a reason for a POSA to modify Hendry to arrive at the claimed invention.

A. Hendry Fails to Teach or Suggest a System that “*receive[s] a request to access a user profile stored at a vehicle.*”

Claims 1 and 11 provide enhanced security for user profiles by requiring authentication and/or verification of a *request to access a user profile* before any access to, or modification of, profile data is permitted. By tying authorization to the specific request to access the user profile, the claimed invention prevents inadvertent and unauthorized changes to profile-stored settings and improves protection of user-specific vehicle preferences that may be reviewed, edited, or updated at the profile level. Ex. 2022 ¶¶ 43, 178.

Hendry does not teach this element. Instead, Hendry describes a process that begins when the vehicle receives a request from an external device to establish a communications link with the vehicle’s communications module, such as via Bluetooth. Ex. 1005 ¶¶ 1, 4-5, 13, 17-18; Ex. 2022 ¶¶ 186, 188-190. Hendry

explains that the communications module “*receives a request from an external device to establish a communications link* with a communications module of the vehicle.” Ex. 1005 ¶ 1; *see also* ¶¶ 4, 5, 13, 17, 18, 27; Ex. 2023 at 83–84, 87, 90–92. That request includes a device identifier and a key. Ex. 1005 ¶ 18. The purpose of this request is solely to initiate a communication session, not to access, view, and/or modify a user profile. Ex. 2022 ¶¶ 193, 214.

After receiving this request, Hendry verifies and/or authenticates the external device, and, if successful, establishes a communications link between the external device and the vehicle. Ex. 2022 ¶ 62. The authentication and/or verification in Hendry is performed solely to determine whether a communications session should be established. Only after the communications link has already been authenticated and established does Hendry initiate any processes relating to user settings. *Id.* ¶¶ 20-25; Ex. 2023 at 89; Ex. 2022 ¶ 188. Those subsequent processes are directed to automatically reinstating previously saved settings, not responding to a received request to access or modify a user profile.

Thus, Hendry receives and authenticates a general request to establish a communications session, not a request to access a user profile. After the communications session is established, Hendry describes the vehicle issuing internal signals to retrieve and reinstate settings. Ex. 1005 ¶¶ 20-25. As Hendry explains this process, “[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. *Id.* ¶ 19. Properly read in context, the communication module first processes the request for establishing a communications link, verifies/authenticates the device and establishes the communications link, and then initiates a separate process to reinstate settings. *Id.* ¶¶ 1, 4, 5, 18, 20-25. As Dr. Martin explains, this “piggybacked” reinstatement operation is initiated by the vehicle after authentication; it is not a request that is received by the vehicle to access a user profile. Ex. 2022 ¶¶ 63, 187–190. Hendry does not disclose receiving a request to access a user profile as a data structure subject to inspection or modification, nor does it authenticate or verify any such request before profile data is accessed. *Id.*

This stands in contrast to the claimed invention, which requires that the request to access the user profile itself be authenticated and/or verified to determine whether the request is authorized. By distinguishing profile access from mere communications connectivity, claims 1 and 11 provide enhanced security that Hendry lacks. Ex. 2022 ¶¶ 202-203, 206. Petitioner does not acknowledge this distinction and does not identify any motivation to modify Hendry’s communications-link process to arrive at the claimed profile-access authorization framework, as explained further below. For at least this reason, Petitioner has failed to demonstrate the obviousness of independent claims 1 and 11.

B. Hendry Fails to Teach or Suggest a System that “*determine[s], 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.*”

Claims 1 and 11 further require determining, 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. This limitation is not satisfied merely by performing authentication or verification at some point in the system. Rather, the claims require that the verification and/or authentication process be performed *in response to the request to access the user profile*, and that the outcome of that process determine whether the request is authorized to access the profile. This sequencing and causal relationship is central to the enhanced security provided by the claimed invention. Ex. 2022 ¶¶ 139–142, 183.

Hendry does not teach this element. In Hendry, any verification or authentication occurs *before* any profile-related processes begin, and is performed solely in response to a request issued by an external device to establish a communications link—not in response to a request to access a user profile. *Id.* ¶ 188; Ex. 1005 at 13, 18–25, 27; Ex. 2023 at 83–84, 95. As discussed above, Hendry authenticates or verifies the external device for the limited purpose of deciding whether to establish a communications session between the external device and the vehicle. Ex. 1005 ¶¶ 18–19, 27; Ex. 2023 at 83–84, 87–89.

Once that communications link is established, Hendry then proceeds to retrieve stored user settings automatically. Ex. 1005 ¶¶ 18–20, 27. Critically, Hendry does not perform any verification or authentication in response to a request to access a user profile, nor does it make any determination that a request is authorized to access profile data. *Id.*; Ex. 2022 ¶ 197–199. The authentication decision in Hendry is complete before any profile access is contemplated, and it does not control or gate access to the user profile itself. *Id.* Hendry also confirms that once a communications link is established, data may be transferred freely between the external device and the vehicle, underscoring that Hendry does not treat profile access as a separately authorized operation. Ex. 1005 ¶¶ 31; Ex. 2022 ¶¶ 193–195.

As a result, Hendry lacks the claimed determination of whether a request is authorized to access the user profile based on a verification and/or authentication process. *Id.* ¶¶ 192, 199. Hendry’s system authenticates a device to communicate, not a request to access profile data. *Id.* ¶¶ 193, 197. This structural and temporal disconnect defeats Petitioner’s attempt to map Hendry’s communications authentication onto the claimed profile-access authorization requirement.

As Dr. Martin explains, a person of ordinary skill in the art would understand Hendry’s authentication as establishing a trusted communications relationship, not as a determination that authorizes access to protected, vehicle-stored profile data or governs subsequent modification or saving of that data. *Id.* ¶ 195. Hendry does not

treat stored settings as profile data whose access requires independent authorization, and its authentication mechanism is functionally exhausted once communications are established. Ex. 2022 ¶¶ 195, 203–204.

Because Hendry does not perform a verification or authentication process in response to a request to access a user profile, and does not determine whether such a request is authorized, it fails to disclose this claim element. *Id.* ¶ 196. Petitioner does not propose any modification to Hendry that would supply this missing authorization determination, and therefore has not established the obviousness of independent claims 1 and 11.

C. Hendry Fails to Teach or Suggest Determining “requested modifications” In Response to an Authorization Determination In Limitation 1[c-3].

Claims 1 and 11 also require that, “in response to determining that the request is authorized to access the user profile,” the system determine “requested modifications” to one or more stored preferences and create an updated user profile. Ex. 2022 ¶ 183. This limitation requires a specific dependency: the system determines requested profile modifications only after—and because—the request has been authorized.

Hendry does not disclose that dependency. In Hendry, after the external device is authenticated to establish the communications link, the user may change vehicle settings “at any given time,” and the system may prompt the user to save those

settings. Ex. 1005 ¶ 31; Fig. 4B; Ex. 2023 at 98-99, 105. Hendry does not disclose that saving modified settings is conditioned on, or performed in response to, any profile-access authorization decision. Ex. 2022 ¶¶ 198.

As Dr. Martin explains, Hendry merely permits a user to change live vehicle settings and optionally save them, without determining those changes as “requested modifications” to a vehicle-stored user profile in response to authorization. Ex. 2022 ¶¶ 197–199. Once Hendry’s external device communications request is authenticated, Hendry permits modification and saving of settings without further authorization analysis. *Id.* Accordingly, Hendry fails to teach or suggest limitation 1[c-3], and therefore fails to render claims 1 and 11 obvious.

D. Hendry Fails to Teach or Suggest a System “*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*” in Claims 6 and 16.

Claims 6 and 16 further narrow claims 1 and 11 by requiring that the one or more processors perform both a verification process and an authentication process, and that the determination that a request is authorized to access the user profile be made in response to successfully verifying the request and successfully authenticating the request. These claims impose a heightened security requirement, in which profile access is permitted only after subjecting the request to access the user profile to multiple, distinct security checks.

Hendry does not teach or suggest this limitation. Ex. 2022 ¶¶ 211–215. As discussed above, Hendry performs at most a single device-level authentication and/or verification step for the limited purpose of establishing a communications link between an external device and the vehicle. Ex. 1005 ¶¶ 1, 4, 18–19, 27. Hendry does not disclose performing both a verification process and an authentication process directed to a request to access a user profile, nor does it disclose combining the results of both processes to determine whether profile access is authorized. Ex. 2022 ¶ 213-215.

More fundamentally, Hendry does not determine that any request is authorized to access a user profile based on the successful completion of verification and authentication. *Id.* Any authentication or verification in Hendry is completed before any profile-related processes begin and is unrelated to profile access. *Id.* Once a communications link is established, Hendry proceeds to retrieve stored settings automatically, without performing additional security checks. *Id.* ¶¶ 197-198.

Claims 6 and 16 therefore impose requirements that are entirely absent from Hendry's system. Petitioner does not propose a POSA would have been motivated to make any changes to the Hendry process, and has therefore failed to demonstrate that claims 6 and 16 are unpatentable.

E. Petitioner Fails to Establish Motivation to Modify Hendry to Arrive at the Claimed Request-Based Profile Authorization Framework.

Petitioner fails to show that Hendry teaches or suggests the claimed invention, and does not identify a motivation to modify Hendry to arrive at the claimed invention. Nor could Petitioner have plausibly done so. The differences between Hendry and the challenged claims are not matters of routine implementation or simple reordering of steps, but instead reflect materially different system purposes and design choices. Ex. 2022 ¶¶ 200–209.

Claims 1 and 11 are directed to managing authorized access to and modification of a user profile stored at a vehicle. The claims require that access to the user profile be subject to authorization, that requested modifications to profile preferences be determined in response to authorization, and that an updated user profile be created in response to those authorized modifications. Ex. 2022 ¶¶ 201–203, 208–209. This structure reflects a system architecture in which stored preferences are treated as protected profile data, and modification of that data is explicitly controlled. Ex. 2022 ¶¶ 147, 159, 201–206.

Hendry is focused on a different issue—it leverages verification and authentication processes solely to establish a trusted communications link between the vehicle and an external device. Ex. 1005 at Abstract, ¶¶ 1, 4, 5, 13, 27, 31; Ex. 2022 ¶¶ 202–203. Once that trust relationship is established, Hendry teaches that

subsequent interactions, including changes to vehicle settings, may proceed without any further authorization check. Ex. 1005 ¶ 31; Ex. 2022 ¶¶ 202-206. Hendry does not disclose using authentication or verification to control or gate access to stored profile data. Ex. 1005 ¶¶ 18–20, 27, 31, 33.

Consistent with this design, Hendry does not identify unauthorized modification of stored settings as a problem, nor does it disclose any mechanism for restricting or re-evaluating authorization to access and modify stored preferences once a communications link has been established. Ex. 2022 ¶¶ 203-206. Hendry performs the initial check to decide whether to establish communications, and considers the issue resolved. *Id.*; Ex. 1005 ¶¶ 31.

As Dr. Martin explains, Hendry does not disclose authorization as being reevaluated for purposes of profile modification. Ex. 2022 ¶ 203. It does not address revocation or contextual limits on access, which confirms that Hendry does not treat modification of stored settings as an access-controlled operation. Ex. 2022 ¶¶ 205–206.

A person of ordinary skill in the art would have had no reason to adapt Hendry’s communications-layer authentication scheme into a mechanism for controlling access to, or modification of, user profile data. Ex. 2022 ¶¶ 204-209. Hendry’s system architecture assumes that once a device has been authenticated to communicate with the vehicle, subsequent interactions—including changing and

saving settings—are permitted without further access control. Ex. 2022 ¶¶ 202-206; Ex. 1005 ¶¶ 31. Hendry neither characterizes stored settings as protected profile data nor suggests that authorization should be reassessed or constrained once the trusted communications link has been established. Ex. 2022 ¶¶ 203-206. Reworking Hendry to impose profile-level authorization would therefore require altering its underlying data-control model, not implementing a predictable or incremental modification. Ex. 2022 ¶¶ 206, 208-209.

Nor can the distinctions between Hendry and the challenged claims be resolved by simply reordering existing steps. Ex. 2022 ¶¶ 208-209. The claims require an authorization-driven workflow in which the outcome of verification and/or authentication governs whether profile data may be accessed and modified, and in which profile updates occur only as a consequence of that authorization. *Id.* Hendry’s system does not disclose or imply such a dependency, and nothing in Hendry would have prompted a person of ordinary skill in the art to introduce it absent impermissible hindsight. Ex. 2022 ¶¶ 207-209.

F. Hendry Fails to Teach or Suggest the Additional Limitations of Dependent Claims 7-8 and 17-18.

Claims 7–8 and 17–18 depend from claims 1 and 11, respectively. For at least the reasons that Hendry fails to teach or suggest core limitations of claims 1 and 11, it necessarily fails to render obvious claims 7–8 and 17–18, which depend from those independent claims. In addition, claims 7 and 17 presuppose a verification process

used to determine whether a request is authorized to access a vehicle-stored user profile, and claims 8 and 18 likewise presuppose an authentication process used for that same authorization determination. Hendry’s verification/authentication is limited to establishing a communications link and does not govern authorization to access or modify a profile. Ex. 2022 ¶¶ 216–221; Ex. 1005 ¶¶ 1, 4, 18–19, 27, 33.

VI. GROUND 3: THE HENDRY-POULSEN COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 3-5 AND 13-15.

Ground 3 challenges only dependent claims and therefore rises or falls with Petitioner’s failure to show Hendry teaches the independent-claim security workflow. Ex. 2022 ¶¶ 233-235, 242-243, 245, 250-251. Because Poulsen is offered only for additional dependent-claim features, it does not cure Hendry’s failure to disclose a request-driven authorization decision governing access to a vehicle-stored user profile. Ex. 2022 ¶¶ 222–224.

Petitioner and its expert rely on Poulsen for the additional limitations of the dependent claims, not on Hendry. That means Ground 3 depends on rewriting Hendry’s architecture to add new profile-synchronization and conflict logic, an alteration Petitioner never argues a POSITA would make. Ex. 2022 ¶¶ 224–226. Petitioner’s asserted rationale speaks only to transmitting and storing profile data externally, not to detecting conflicts among profile instances, overwriting only conflicted preferences, or selectively reconciling conflicts. *Id.* ¶ 226.

A. Poulsen Fails to Teach or Suggest “Determining Whether Any Conflicts Exist” Between Updated Preferences and Local Preferences.

Poulsen does not teach or suggest the additional limitations of claims 3–5 and their method counterparts, claims 13–15, which require determining whether conflicts exist between updated preferences in an updated user profile and previously stored local preferences at a mobile device, server, or other vehicle, and—where conflicts exist—resolving those conflicts through overwriting or selective reconciliation. Ex. 2022 ¶¶ 227

Specifically, claims 3 and 13 involve determining “whether any conflicts exist between the user’s updated preferences and the preferences stored at the mobile device, server, or other vehicle specified in claim 2. Claims 4 and 14 further require overwriting the conflicted preferences on the mobile device, server, or other vehicle with the user’s updated preferences at the vehicle. And claims 5 and 15 offer an alternative approach involving “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.” Ex. 2022 ¶¶ 234, 242, 245.

Poulsen contemplates providing a prompt when saving data that may already exist, but Poulsen does not describe determining whether any conflicts exist between updated preferences and existing preferences, and it does not involve resolving

conflicting preferences. Instead, Poulsen’s disclosure is limited to prompting a user to confirm whether to overwrite previously stored profile data. Ex. 1006 ¶ 87. That prompt occurs regardless of whether the underlying profile data has changed and does not require any comparison between the contents of an existing profile and the contents of a profile to be saved. Ex. 2022 ¶¶ 227–240.

As Dr. Martin¹ explains, a POSITA would understand Poulsen’s saving mechanism to be analogous to a conventional “Save As” function, in which a user is prompted to confirm whether an existing data file should be overwritten based solely on the existence of a file with the same identifier—not based on a determination that any differences or conflicts exist between the two versions. Ex. 2022 ¶¶ 227, 235–237. Such a confirmation mechanism does not entail detecting conflicts, identifying inconsistent preferences, or determining whether any differences exist at all.

Dr. Martin provides an illustrative example where a user changes a setting only to subsequently revert to the previous setting. Ex. 2022 ¶ 238. Poulsen’s system would nevertheless ask the user whether to overwrite the existing stored profile. *Id.* This demonstrates that Poulsen’s prompting mechanism operates

¹ Patent Owner’s expert Dr. Paul Martin’s CV (Ex. 2021) and corresponding Declaration (Ex. 2022 ¶¶ 1–40) illustrate his qualifications to opine from the perspective of a POSITA.

independently of any determination that conflicts or differences exist and therefore fails to teach or suggest the limitation of determining whether any conflicts exist between updated preferences and local preferences, as required by claims 3 and 13. Ex. 2022 ¶¶ 236–240.

More broadly, Poulsen never describes identifying conflicting preferences, comparing profile data to detect conflicts, or determining whether conflicts exist between updated and locally stored preferences. Poulsen does not even use the word “conflict.” Instead, Poulsen relies on user input to overwrite saved data, without any automated or logical assessment of whether stored preferences conflict and require reconciliation. Ex. 1006 ¶ 87; Ex. 2022 ¶¶ 227, 239.

Because Poulsen fails to teach or suggest determining whether conflicts exist between updated preferences and local preferences, Hendry in view of Poulsen fails to render claims 3 and 13 obvious. Ex. 2022 ¶ 240. And because Poulsen likewise fails to teach overwriting conflicted preferences or selectively reconciling conflicts, it also does not supply the additional limitations of claims 4–5 and 14–15. Ex. 2022 ¶¶ 242–247.

B. Petitioner Fails to Establish Motivation to Modify Hendry Based on Poulsen to Add Conflict Detection or Resolution.

Petitioner’s proof additionally fails with respect to claims 3–5 and 13–15 because it fails to provide a motivation to modify Hendry based on Poulsen to arrive at the inventions of these claims. Ex. 2022 ¶¶ 241, 244, 247. Petitioner sets forth a

single motivation to modify Hendry based on Poulsen for all the claims it challenges in Ground 3. Petition at 57–60. But this motivation to combine focuses exclusively on the elements of claims 2 and 12, without addressing or considering any additional elements of the other claims challenged in Ground 3. Ex. 2022 ¶ 226.

It is Petitioner’s burden to identify “with particularity” the evidence that “a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so.” *Apotex Inc. v. Wyeth LLC*, IPR2014-00115, Paper 94 at 11 (Apr. 20, 2015). Petitioner has failed to satisfy this burden.

As explained above, claims 3–5 and 13–15 recite specific requirements directed to conflict detection and resolution between multiple stored instances of a user profile following an update. Petitioner’s asserted motivation to combine does not address these requirements. And nothing in Hendry would have prompted a POSITA to add conflict detection or selective reconciliation. Hendry does not identify conflicting profile instances as a technical problem, does not maintain multiple authoritative profile copies whose contents could diverge, and retrieves/overwrites settings without any disclosure of conflict management. Ex. 1005 ¶ 31; Ex. 2022 ¶ 228.

Petitioner argues that a POSA would have been motivated to “transmit and save profiles to an external location” and that a POSA would have considered this “a simple modification” involving servers and mobile devices and “conventional techniques” such as the Internet and Bluetooth. *Id.* at 59–60. Even if accepted at face value, this asserted motivation addresses only transmission and storage of profiles, not the identification or resolution of conflicts between different profile instances. Petitioner does not offer any motivation to modify Hendry in view of Poulsen to provide for conflict detection, overwriting of conflicted preferences, or selective reconciliation as required by claims 3–5 and 13–15. Ex. 2022 ¶ 226.

Instead, Petitioner simply alleges that Poulsen discloses those elements. As discussed above, that assertion is incorrect, and in any event does not supply the required motivation to modify Hendry. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (“[A] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art.”). Dr. Martin explains that Petitioner’s analysis is classic hindsight: it starts with the claim language and then asserts—without any teaching in Hendry or Poulsen—that ‘the processors executing instructions’ would perform the claimed conflict functions. Ex. 2022 ¶ 229. That is not an articulated reason to modify Hendry; it is reconstruction using the claims as a roadmap. Without a motivation to modify, Petitioner’s analysis is purely hindsight driven—an effort to find disclosure of

claimed elements rather than a prior art-based motivation to arrive at the claimed invention. *Innogenetics, N.V. v. Abbott Lab 'ys*, 512 F.3d 1363, 1373 (Fed. Cir. 2008) (finding a lack of explanation as to why a POSA would have found claims obvious in light of a combination of references unhelpful “in avoiding the pitfalls of hindsight that belie a determination of obviousness”); *see also ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1327 (Fed. Cir. 2012) (finding conclusory motivation to combine “not sufficient and [] fraught with hindsight bias”).

The hindsight pitfall is particularly relevant given the very different focuses of Poulsen and Hendry (and the '243 patent). Poulsen focuses on a generalized profile and meta-configuration framework that allows users to create, link, store, and apply collections of attributes to content in a variety of environments. Ex. 1006 ¶¶ 2, 4-5, 35, 82; Ex. 2022 ¶¶ 75-76. Poulsen contemplates vehicles as just one of many possible environments for application of its systems. Hendry, on the other hand, is focused on establishing an authorized communication link between a mobile device and a vehicle and then automatically restoring locally stored vehicle settings. Ex. 1005 ¶¶ 17-25. Neither reference is directed to detecting conflicts between multiple stored profile instances or selectively reconciling those conflicts following an authorized profile update at the vehicle. Ex. 2022 ¶¶ 225–229. Without a motivation to modify Hendry with Poulsen, Petitioner is left with only a hindsight-driven argument to yield the claimed invention. *Id.*

For at least this reason, Petitioner fails to demonstrate the obviousness of the claims 3–5 and 13–15. *Id.*

C. Poulsen Fails to Teach Dual Verification and Authentication Used to Authorize Access to a User Profile in Claims 6–7 and 16–17.

Petitioner also fails to demonstrate the obviousness of claims 6–7 and 16–17. Claims 6 and 16 require performance of both a verification process and an authentication process to determine whether a request to access a user profile is authorized, while claims 7 and 17 further specify particular verification techniques such as biometric recognition or identification of a mobile device.

First, Petitioner does not suggest that a POSITA would have been motivated to modify Hendry based on Poulsen. Petitioner contends that “Hendry in view of Poulsen” renders these claims obvious, but its analysis is limited to generalized statements about security techniques that Poulsen mentions. Pet. at 71. That is not sufficient. As discussed, an obviousness analysis requires more than identifying allegedly known security techniques; it requires explaining how and why a POSITA would modify the prior art system at issue—here, Hendry—to perform both verification and authentication in response to a request to access a user profile at a vehicle. *KSR*, 550 U.S. at 418; *Innogenetics*, 512 F.3d at 1373; *ActiveVideo*, 694 F.3d at 1327.

As discussed above, Hendry does not disclose a system or method as required by claims 6–7 or 16–17 because Hendry does not disclose the step of “receiv[ing] a

request to access a user profile stored at a vehicle,” or “performing at least one of a verification process or an authentication process in response to the request [to determine] whether the request is authorized to access the user profile.” Petitioner’s Ground 3 arguments do not propose any modification to Hendry to supply these missing steps. Ex. 2022 ¶ 248. Its expert, Mr. Denning, confirmed this at deposition when he agreed that, with respect to claim 6, Poulsen was “more of the same” and he was not proposing changes to Hendry based on Poulsen. Ex. 2023 at 112; Ex. 2022 ¶ 231. Where, as here, Petitioner does not actually rely on Poulsen to modify Hendry for these limitations, there is no articulated combination rationale, and Poulsen cannot supply the missing “authorization-to-access-profile” features absent from Hendry. Ex. 2022 ¶¶ 230–232. Petitioner’s Ground 3 arguments instead rely on the assertion that Poulsen states that stored profiles “can be encrypted and/or locked” and that security “may include one or more authentication methods and technologies such as biometric identification.”

Even if Petitioner had argued that a POSITA would have been motivated to modify Hendry based on Poulsen, the result would not have yielded the claimed invention. Poulsen does not describe a vehicle receiving a request to access a user profile, and does not describe performing both verification and authentication in response to such a request. Rather, Poulsen discusses optional security features in

the abstract as part of a generalized profile framework that may be used across many different environments. Ex. 1006, Abstract ¶¶ 35, 82; Ex. 2022 ¶¶ 230–232.

Further, Petitioner never explains why a POSITA would look to Poulsen to modify Hendry with respect to authentication and verification techniques. As discussed above with respect to claims 3–5 and 13–15, Poulsen is focused on a generalized profile and meta-configuration framework applicable across many environments, whereas Hendry is focused on establishing an authorized communications link and thereafter reinstating locally stored vehicle settings. Petitioner does not articulate any reason why a POSITA would import Poulsen’s generalized, optional security concepts into Hendry’s system—much less why a POSITA would do so in a way that results in the specific dual-process authentication and verification scheme recited in claims 6–7 and 16–17. Ex. 2022 ¶¶ 230–232, 248–252.

D. Petitioner Fails to Establish a Reasonable Expectation of Success for the Asserted Hendry–Poulsen Modifications.

Finally, Petitioner also fails to allege—much less demonstrate with particularity—that a POSA would have had a reasonable expectation of success in making any of the unidentified and unsupported modifications to Hendry based on Poulsen to arrive at the inventions of claims 2–7 and 12–17. Dr. Martin explains that the alleged “modifications” are not described at the architectural level needed to assess feasibility, much less success. Ex. 2022 ¶ 226. Petitioner never identifies

what Hendry component(s) would perform the added conflict comparison, how conflicts would be detected across separate profile instances, or how reconciliation rules would be applied within Hendry’s component-specific datastores and workflows. *Id.* A petition that “does not show, let alone with the particularity required by statute, a reasonable expectation of success” fails to establish obviousness by a preponderance of the evidence. *Juniper Networks, Inc. v. Correct Transmission, LLC*, IPR2021-00682, Paper 26 at 26, 35 (PTAB Oct. 3, 2022).

Although Petitioner includes headers invoking “reasonable expectation of success” and summarily asserts that “[a] POSA would have been motivated to apply, and had a reasonable expectation of success,” (Pet. at 57), Petitioner’s analysis addresses only its alleged motivation to combine—not whether a POSA would reasonably expect those modifications would be successful. For example, Petitioner never explains—claim by claim—how a POSA would implement (i) conflict detection between “updated preferences” and a ‘local user profile’ at a remote destination, (ii) overwriting only “conflicted ones” of local preferences, or (iii) a “reconciliation process” that selectively determines which conflicts to overwrite. Nor does it explain how Hendry would be modified to perform both verification and authentication in response to a profile-access request, as claims 6 and 16 require. Ex. 2022 ¶ 226. Nowhere does Petitioner analyze reasonable expectation of success on a claim-by-claim basis for claims 2–7 or 12–17.

Instead, the Petition and accompanying declaration rely on conclusory assertions of success without explanation. That omission is especially stark given the changes Petitioner implicitly needs. As Dr. Martin explains, repurposing Hendry’s one-time communications pairing into an authorization state that governs later modification of stored vehicle preferences would require design choices Hendry never contemplates—what terminates authorization (loss of link, vehicle shutdown, user exit), and how the system prevents unauthorized modification if device control changes. Ex. 2022 ¶ 206. But a conclusory assertion with no explanation is inadequate to support a finding of obviousness. *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1359 (Fed. Cir. 2019). Because Petitioner fails to articulate a reasonable expectation of success with the required particularity for the inventions recited in Ground 3, its obviousness challenge fails for this additional, independent reason.

VII. GROUND 4: THE HENDRY–ROVIK COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 9–10 AND 19–20.

Ground 4 challenges only dependent claims 9–10 and 19–20. But Petitioner does not attempt to cure the independent-claim defects that defeat Ground 2. For that reason alone, Ground 4 fails. Ex. 2022 ¶ 274. In any event, Petitioner’s Hendry–Rovik combination independently fails to teach the additional “template” limitations of claims 9–10 and 19–20, and Petitioner offers no non-hindsight

reason—nor any coherent implementation pathway—for modifying Hendry to adopt Rovik’s fundamentally different, server-centered framework. Ex. 2022 ¶¶ 255–268.

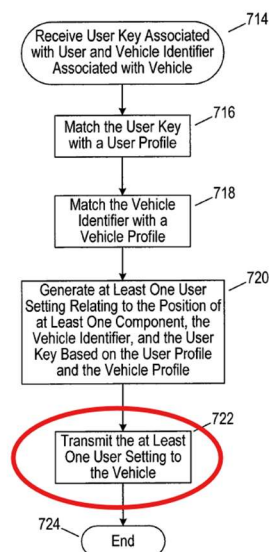
A. Hendry-Rovik Fails to Teach or Suggest “*wherein the user profile is based on a template for the one or more preferences, and the updated user profile is created relative to the template.*”

Claims 9 and 19 are not merely about transmitting or applying settings. They require that the vehicle-resident user profile recited in claims 1 and 11 (and the “updated user profile” created at the vehicle) is based on a template for the preferences, and that the update is created relative to that template. Ex. 2022 ¶¶ 10–16, 18–19. These limitations impose a structural and operational requirement that the vehicle must maintain a templated profile organization for preferences and create profile updates in a manner that preserves and operates relative to that template. Ex. 2022 ¶¶ 256–257.

Rovik does not disclose any such vehicle-side templated profile structure or templated update operation. Rovik’s “standardized” constructs exist at a remote server as part of a computation framework that combines user attributes with vehicle-profile constraints to generate new vehicle-specific settings for a vehicle the user has not previously driven. Ex. 1007 9:14–17, 13:2–13; Ex. 2022 ¶¶ 9–12, 15–18. As Dr. Martin explains, Rovik’s “standardization” is a server-side reference model used to generate different vehicle-specific outputs; it is not a vehicle-resident template for storing and updating a profile. Ex. 2022 ¶¶ 262–268.

Rovik stores “standardized” user profiles at a remote server to define abstract user attributes (e.g., eye point, hip point, arm length) and settings. Ex. 1007 at 9:13–37; Ex. 2022 ¶¶ 262-263, 267-68. These user profiles are never sent to vehicles. Ex. 2022 ¶¶ 270-271. Instead, the server calculates settings tailored to a new vehicle based on application of a vehicle-specific model profile to the abstract attributes and settings to account for differences between vehicles such as feature availability and interior geometries. Ex. 1007 at 3:18–26; 7:48–8:59; 9:40–43; 9:59–64; 10:8–10; 13:2–6; Ex. 2022 ¶¶ 260-266. For example, Rovik emphasizes that some vehicles lack automatically adjustable components and that available settings depend on system availability and vehicle type. Ex. 1007 at 8:7–10, 8:32–39; 8:55–59; Ex. 2022 ¶¶ 260-265. And Rovik explains that it is only those newly generated vehicle-specific *settings* that are transmitted to the vehicle after this process. Ex. 1007 at 13:10–13; Ex. 2022 ¶¶ 261-263, 268-270.

Notably, Rovik does not describe that these vehicle-specific settings are sent in a particular format, nor with an identifier of the user. Instead, as shown in Figure 9 and confirmed in the corresponding discussion, Rovik describes transmitting calculated settings to the vehicle (e.g., component positions), not transmitting a vehicle-resident “user profile” data structure organized according to a template. Ex. 1007 at 13:10-13; Ex. 2022 ¶¶ 270-271.



A POSA would not consider bare settings sent by the server to the vehicle to be a user profile based on a template. Ex. 2022 ¶¶ 270-271. And even if Petitioner’s combination of Rovik and Hendry was proper, Hendry’s settings would at most reflect vehicle-specific outputs calculated by Rovik, not “based on a template for the one or more preferences, and the updated user profile is created relative to the template.” Therefore, Hendry in view of Rovik fails to teach or suggest the additional features of claims 9 and 19. Ex. 2022 ¶¶ 256-273.

B. Hendry–Rovik Fails to Teach or Suggest “*wherein the template is a global standard template that is common among at least two vehicle manufacturers.*”

Claims 10 and 20 depend from claims 9 and 19 respectively. Because Hendry in view of Rovik fails to teach or suggest claims 9 and 19, Hendry in view of Rovik likewise fails to teach the additional features of claim 10 and 20. Ex. 2022 ¶ 279.

Indeed, claims 10 and 20 provide more specificity in that the template of claim 9 and 19 is a global standard template that is common among at least two vehicle manufacturers. Rovik uses different vehicle profiles to convert its server-based abstract attributes and settings into vehicle specific settings. Ex. 1007 at 9:54-64, 13:2-12. That disclosure underscores the opposite of a “global standard template” shared across manufacturers: Rovik teaches that vehicle-to-vehicle variability requires vehicle-specific constraints and server-side translation. Ex. 2022 ¶¶ 260–265, 275–278. Therefore, what is ultimately sent to vehicles (including Hendry’s vehicle) by Rovik is necessarily tailored to a particular vehicle’s attributes rather than derived from a common, cross-manufacturer template. Ex. 2022 ¶¶ 275-279. Even in the combination of Hendry and Rovik, the user profile stored at the vehicle (per claim 1) would be based on vehicle specific settings, not “a global standard template that is common among at least two vehicle manufacturers.” Therefore, Hendry in view of Rovik fails to teach or suggest the additional features of claims 10 and 20. Ex. 2022 ¶¶ 275-279.

C. Petitioner Fails to Establish a Motivation to Modify Hendry Based on Rovik to Implement a Vehicle-Resident Template-Based Profile Architecture.

Not only does Rovik fail to teach or suggest the elements of claims 9-10 and 19-20—elements that Petitioner does not even contend Hendry suggests—Petitioner also fails to identify any reason why a person of ordinary skill in the art would have

been motivated to modify Hendry in view of Rovik to arrive at the claimed invention. Petitioner’s assertion that Rovik’s profiles “could readily be transferred and applied” is insufficient. Pet. at 103. A showing that something *could* be done does not explain *why* a POSITA would alter Hendry’s in-vehicle architecture in the manner required by claims 9–10 and 19–20.

Hendry involves a local, in-vehicle architecture in which authenticated external devices trigger reinstatement of settings retrieved from data stores within a single vehicle. Ex. 2022 ¶¶ 259, 265–266. Consistent with that architecture, Hendry does not contemplate cross-vehicle portability, server-side processing, or translation of user attributes into vehicle-specific outputs. Ex. 2022 ¶ 259.

Rovik addresses a different problem and proposes a fundamentally different system. Rovik recognizes that different vehicles may have different interior geometries, system capabilities, and available settings, such that preferences may not directly map from one vehicle to another. Ex. 1007 at 8:7–10; 8:32–39; 8:55–59. Consistent with that premise, Rovik describes a server-side computational process for generating new, vehicle-specific settings by combining user attributes with vehicle specific profiles that reflect the vehicle’s relative geometry and capabilities. Ex. 1007 at 2:6–23; 8:66–10:25; 12:50–13:13, Fig. 9 (steps 720–722). Rovik then transmits only the calculated, vehicle-specific settings to the vehicle. Ex. 1007 at 2:6–23; 13:10–13; Fig. 9 (step 722). Rovik’s “standardized” user profile thus

functions solely as a server-side computational reference and is not transmitted to, stored at, or used by the vehicle as a template for structuring a local user profile. Ex. 2022 ¶¶ 262–268, 270–271.

Given these teachings, a POSITA would not have been motivated to modify Hendry to use Rovik’s standardized user profile as a template for the user profile of Hendry, as required by claims 9–10 and 19–20. Ex. 2022 ¶¶ 263–268. In fact, Rovik ties its standardized user profiles to server-side translation to create divergent vehicle-specific settings, thereby teaching that direct transfer of preferences without such translation would be unreliable. Ex. 2022 ¶¶ 260–265; Ex. 1007 at 8:32–39; 8:55–59; 9:14–10:25; 13:2–13. Rovik therefore teaches away from using a standardized profile as a vehicle-resident template. Ex. 2022 ¶¶ 264–265.

Petitioner also fails to explain how Rovik’s server-side computation framework would be integrated with Hendry’s distributed, component-module architecture to yield a “user profile stored at a vehicle” that is “based on a template” and updated “relative to the template,” as required by claims 9–10 and 19–20. Ex. 2022 ¶¶ 265–266. Such a modification would require a substantial redesign of Hendry’s system, yet Petitioner identifies no technical reason why a POSITA would undertake that redesign rather than follow Rovik’s disclosed approach of generating vehicle-specific settings at a server and transmitting only those settings to the vehicle. *Id.*

Accordingly, Petitioner has not shown a motivation to combine Hendry and Rovik in a manner that would yield the claimed template-based user profiles required by claims 9–10 and 19–20, and Ground 4 fails for this additional reason.

VIII. GROUND 5: SINGH FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 1, 6–7, 11, AND 16–17.

Petitioner fails to prove its obviousness arguments in Ground 5, which challenge claims 1, 6-7, 11, and 16-17. As discussed with respect to Hendry, the claims of the '243 patent are concerned with securing user profiles, including controlling whether and how those profiles may be accessed and modified. And Singh is directed to a system for determining whether to allow a driver to access and operate a vehicle. Because Singh, like Hendry, does not describe a process for receiving a request to access a user profile, and determining—by verification and/or authentication performed in response to that request—whether the request is authorized before allowing access to and modification of the profile, it fails to render the claimed invention obvious. Ex. 2022 ¶¶ 280–288.

A. Singh Fails to Teach or Suggest a System that “*receive[s] a request to access a user profile stored at a vehicle.*”

Singh fails to teach or suggest “receiving a request to access a user profile” as required by independent claims 1 and 11. As discussed with respect to Hendry, the claims are structured around a request-based security framework in which access to a user profile begins only after the system receives a request to access a user profile.

The “request” is therefore a discrete, system-level event directed specifically to accessing a user profile, and it precedes and triggers the authorization determination recited in the claims. Ex. 2022 ¶¶ 280–283. The Petition does not identify any such request in Singh, and Singh does not describe such a request.

Petitioner argues that Singh discloses “a multi-factor authentication/verification process *to initiate a request to access a user profile*,” but never specifies what it considers to be the “request to access a user profile” or what component of the system “receives” the request. See Pet. at 83-84 (emphasis added). The Petition’s framing confirms that the alleged “request” is not an independent event at all, but is instead purportedly created by the verification/authentication process itself. This is because Singh never describes any such request. Instead, Singh discloses a sequence in which a driver enters a password and scans a fingerprint, the system identifies the driver, the vehicle allows the driver to open the door, and then starts the engine. After this process is completed, the vehicle initiates a process to apply stored settings corresponding to the driver. Ex. 1008 ¶¶ 38–41; Ex. 2022 ¶¶ 281–283.

Petitioner’s reference to “a multi-factor authentication/verification process” involving password and fingerprint authorization processes does not resolve this failure. Pet. at 83. Singh confirms these actions are part of a process for unlocking the vehicle to secure entry. In the ’243 claims, by contrast, profile access is

independently driven through an authorization determination specific to the request to access the profile. Because Singh never receives a request to access a user profile, it cannot satisfy the first limitation of claims 1 and 11. Ex. 2022 ¶¶ 280–284.

Petitioner neither acknowledges that Singh fails to teach this requirement, nor contends a POSA would have been motivated to make any changes to the Singh system in order to arrive at the claimed invention. As explained further below, a person of ordinary skill in the art would have had no reason to modify Singh in this manner. Ex. 2022 ¶¶ 291-296. Petitioner has therefore failed to demonstrate that claims 1 and 11 are unpatentable over Singh.

B. Singh Fails to Teach or Suggest a System that “*determine[s], 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.*”

Singh also fails to teach or suggest a system or method that “determine[s], 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 explained above, the claims require a system in which a request to access a user profile is received and then evaluated to determine whether that request is authorized. The verification and/or authentication processes are to be performed for the specific purpose of deciding whether access to the user profile should be granted. This reflects a security architecture in which access to profile data is conditional and subject to authorization. Ex. 2022 ¶¶ 285–288.

Singh does not disclose any such determination. Singh uses a password and fingerprint solely to decide whether to permit entry into and operation of the vehicle. Ex. 1008 at ¶¶ 38-39; Fig. 3. Singh expressly frames this as a stepwise vehicle-entry process, in which the “first step” is entry of a password, which causes a door to the fingerprint sensor to open. *Id.* In the “second step,” the user provides a fingerprint impression that the vehicle compares to stored data. *Id.* If the password does not match in the first step, or fingerprint impression does not match in the second step, the process does not proceed to the next step. *Id.* at ¶¶ 39-40. If the passcode and finger impression steps are successfully completed, the door is unlocked. *Id.* at ¶ 40. And once the driver opens the door, the Singh system starts the engine. *Id.* Singh then explains that only after “the verification has been performed and the vehicle started” does it load the essential vehicle features corresponding to the driver’s stored preferences. *Id.* at ¶ 41.

Critically, Singh does not perform any verification or authentication process “in response to the request” to access a user profile, because Singh does not teach or suggest a request to access a user profile in the first place. Ex. 2022 ¶ 294. The Petition’s position compounds this failure by asserting that Singh’s “multi-factor authentication/verification process” is what “initiate[s]” a request to access a user profile,”—meaning that the alleged request is generated by the verification/authentication process itself. Pet. at 83. Under that theory, verification

and authentication cannot logically be performed “*in response to*” the request, as required by the claims. Ex. 2022 ¶¶ 286–288. Petitioner’s own framing thus defeats element 1[c-2]. If authentication “initiates” the request, authentication necessarily precedes the request and cannot be performed “in response to” it. Pet. at 83; Ex. 2022 ¶¶ 286–288.

Any verification or authentication steps described in Singh occur before—and independently—of any processes related to applying stored settings. As a result, unlike in the claims, Singh does not gate profile access by its own authorization determination. Ex. 2022 ¶¶ 289–295.

The Petition attempts to collapse authentication of a person seeking to enter a vehicle into authorization of a request to access a user profile. That approach is inconsistent with both the ’243 claim language and Singh’s disclosure. Determining whether to allow someone to open a vehicle door is not the same as determining whether a request to access a user profile is authorized. Singh itself demonstrates this distinction: the password/fingerprint checks are tied to vehicle entry and engine start, and only after those checks does Singh initiate any process for loading the driver’s stored settings. Ex. 2022 ¶¶ 289–294; Ex 1008 ¶¶ 38-41.

Petitioner does not offer any reason to modify the system or process in Singh to perform an authentication or verification process in response to a request to access a user profile and determine whether such access should be granted. This

independent deficiency further confirms that Singh does not render claims 1 and 11 obvious, particularly where Singh's disclosed architecture provides no motivation to introduce a request-based authorization framework for accessing user profile data. Ex. 2022 ¶¶ 291–296.

C. Petitioner Fails to Establish a Motivation to Modify Singh to Add a Request-Based Profile Authorization Framework.

Singh does not teach or suggest the invention of claims 1 and 11, and, as with Hendry, Petitioner does not propose a motivation to modify Singh to arrive at the claimed invention. And like Hendry, no such motivation exists.

Singh reflects a deliberate architectural choice to have authentication and verification control vehicle entry and operation, not access to and modification of stored user profile data. Ex. 2022 ¶¶ 291-296. Singh is expressly motivated by concerns about unauthorized vehicle use, and it addresses those concerns by requiring successful completion of a password entry and fingerprint scan before unlocking the vehicle and starting the engine. Ex. 1008 ¶¶ 2–4, 38–40; Ex. 2022 ¶¶ 291-295. Once those steps are completed and the vehicle is started, Singh initiates a features-loading process to apply stored driver preferences. Ex. 1008 ¶¶ 39–41; Ex. 2022 ¶¶ 292-295. Nothing in Singh suggests that access to profile data itself presents a separate security concern, or that such access should be conditioned on a request-specific authorization determination. Ex. 2022 ¶¶ 292-296.

To the contrary, Singh assumes that once a driver has been authenticated for vehicle entry, subsequent interactions with profile data are permitted. Ex. 2022 ¶¶ 293-296; Ex. 1008 ¶ 62. Singh allows drivers to modify and save preference files through a graphical user interface and automatically saves those changes when the vehicle is turned off, without performing any further authorization analysis. Ex. 1008 ¶ 62; Ex. 2022 ¶¶ 293-296. Singh does not describe authentication as a persistent or scoped authorization state, nor does it disclose evaluating whether individual requests to access and modify profile data remain authorized after the vehicle has been opened. Ex. 2022 ¶¶ 294-295.

Dr. Martin explains that, as with Hendry, Singh's system architecture assumes that once a driver has been authenticated for entry and operation, subsequent interactions—including changing and saving settings—are permitted without further access control. Ex. 2022 ¶¶ 293-296. Singh authenticates a driver, not a request, and it does not disclose or suggest a request-driven access-control model for profile data. Ex. 1008 ¶¶ 38-41; Ex. 2022 ¶¶ 280-288, 294-296. Modifying Singh to perform verification or authentication in response to a request to access a user profile—as required by the claims—would require introducing an additional access-control layer that Singh neither teaches nor suggests. Ex. 2022 ¶¶ 294-296.

Nor does Singh identify any technical problem related to unauthorized profile access or modification that would motivate such a redesign. *Id.* Singh's silence on

profile-level authorization reflects a design assumption that profile changes do not require independent security controls once a driver has been authenticated to use the vehicle. Ex. 2022 ¶¶ 293-296. In this respect, repurposing Singh's password and fingerprint mechanisms to authorize requests to access or modify user profiles would not be a routine or obvious variation but instead would require rearchitecting Singh's system in a manner inconsistent with its stated objectives and disclosed operation. Ex. 2022 ¶¶ 291-296.

Accordingly, a POSA would not have been motivated to modify Singh to implement the request-based profile access and authorization framework recited in claims 1, 6-7, 11, and 16-17. Ex. 2022 ¶¶ 291-297.

D. Singh Fails to Teach the Additional Limitations of Claims 6-7 and 16-17.

Claims 6 and 16 require performance of both an authentication and verification process to determine whether a request to access a user profile is authorized. Claims 7 and 17 further specify the methods by which verification is performed.

As discussed with respect to claims 1 and 11, Singh neither suggests a system or process that receives a request to access a user profile, nor performs an authentication or verification process in response to such a request for purposes of authorizing profile access. It necessarily follows that Singh does not teach the additional elements of claims 6-7 and 16-17. Ex. 2022 ¶¶ 298-299. Thus, for at

least the reasons discussed with respect to claims 1 and 11, Petitioner has failed to demonstrate the obviousness of claims 6-7 and 16-17 based on Singh.

IX. GROUND 6: THE SINGH–CAZANAS–FORSTALL COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 2–8 AND 12–18.

Petitioner’s arguments in Ground 6, which involves claims dependent on the independent claims addressed in Ground 5, do not attempt to resolve the issues identified with respect to Ground 5. Thus, Petitioner’s arguments in Ground 6 fail for at least the reasons discussed with respect to Ground 5. Ex. 2022 ¶¶ 300–314.

A. Petitioner Fails to Establish a Motivation to Combine Singh, Cazanias, and Forstall to Arrive at the Claimed Inventions.

Petitioner asserts that a POSA would have been motivated to combine Singh, Cazanias, and Forstall because they purportedly fall within the same field and address the same general problem of managing “vehicle-related user data.” Pet. at 89-90. That assertion, however, rests on an overly generalized framing that glosses over the different technical focuses and architectures of the cited references, and fails to explain why or how a POSA would have combined all three references to arrive at the claimed invention. Ex. 2022 ¶¶ 302–307.

Singh, Cazanias, and Forstall address distinct problems at different system layers, using different mechanisms and design assumptions. Singh is directed to identifying a driver for purposes of controlling vehicle access and operation, and thereafter reinstating a locally stored vehicle profile. Ex. 1008 ¶ 3-4. Cazanias is

directed to server-based portability of driver profiles across vehicles, using telematics units and centralized storage to facilitate transferring profiles between different vehicles. Ex. 1009 at 1:15–40. Forstall, by contrast, is directed to synchronizing data items between a mobile device and a vehicle device, primarily for navigation data, contacts, and other general information, and includes user-configurable synchronization and conflict-resolution preferences. Ex. 1010 at Abstract, ¶¶ 3-9. These references do not provide “complementary teachings,” as Petitioner asserts; rather, they are architecturally and functionally distinct systems optimized for different objectives. Ex. 2022 ¶¶ 305–309.

Critically, Petitioner never articulates a concrete reason why a POSA would have looked to *Forstall’s* mobile-device synchronization framework to modify either *Singh’s* access-control and profile-reinstatement processes or *Cazanas’s* server-centric profile transfer system—much less why a POSA would have done so in a way that introduces the request-based authorization gate required by the claims. Ex. 2022 ¶ 303-308. Forstall does not address secure access to a vehicle-stored user profile, nor does it concern authorization of a request to access a user profile—it lets the user decide to synchronize and reconcile data differences. Ex. 1010 ¶¶ 82-83, 92, 97-99, Petitioner’s rationale thus reflects hindsight driven by the claims, rather than an art-based motivation grounded in the prior art. Ex. 2022 ¶¶ 306–313.

Petitioner’s reliance on broadly-drawn, high-level statements that the references are in the “same field” or address “user convenience” is insufficient. The law requires more than drawing a large box that captures numerous prior art references, and instead requires “an articulated reasoning with some rational underpinning” as to why a POSA would have combined the particular teachings of the references in the manner claimed. *KSR*, 550 U.S. at 418. Here, Petitioner does not explain why a POSA seeking to improve Singh’s vehicle-based profile management would import Forstall’s device-to-device synchronization logic—originally developed for sharing navigation and contact data—into a system concerned with authorizing vehicular access, operation, and loading of user settings. Ex. 2022 ¶¶ 306–309.

Nor does Petitioner explain how a POSA would have reasonably expected success in integrating these disparate systems without fundamentally altering their respective architectures. Singh’s system operates around reinstating locally stored settings after a driver has already been authenticated for vehicle access and operation; Cazan’s system operates around remote storage and retrieval of profiles via telematics; and Forstall’s system operates around bidirectional synchronization between devices with user-controlled conflict rules. Ex. 2022 ¶¶ 308–312.

Petitioner’s argument also fails because it does not explain how a POSA would actually combine these three references into a single, coherent system or

method. Instead, Petitioner treats the references as a menu of interchangeable features, selectively invoking aspects of each without identifying the underlying system architecture or method flow that would govern the combined system. Ex. 2022 ¶¶ 308–312.

At no point does Petitioner identify with any specificity which system properties or method steps are retained from Singh, which are imported from Cazanias (and where in the Singh process they are imported), and which additional properties or steps are taken from Forstall (and how those fit into the unarticulated combination of Singh and Cazanias). For example, Petitioner does not explain (1) how Singh’s locally stored vehicle user profile would be modified to incorporate Cazanias’s server-based profile transfer mechanisms; (2) 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; or (3) 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. Ex. 2022 ¶¶ 310–313.

Instead, Petitioner’s theory proceeds by plucking individual features from each reference that are recited the claims. Such an approach amounts to hindsight-driven reconstruction, not a reasoned explanation of obviousness. Ex. 2022 ¶ 312.

In short, Petitioner’s motivation-to-combine analysis relies on generalities rather than specifics. It does not explain why a POSA would have landed upon and combined all three references, or how such a combination would yield the claimed systems and methods. For this additional reason, Petitioner has failed to demonstrate that claims 2-8 and 12-18 are unpatentable based on Ground 6. Ex. 2022 ¶ 313.

B. The Singh–Cazanas–Forstall Combination Fails to Teach Dual Verification and Authentication Used to Authorize Access to a User Profile In Claims 6–8 and 16–18.

Petitioner also fails to show that the Singh-Cazanas-Forstall combination teaches or suggests claims 6–8 and 16–18. They require performing both a verification and authentication process in response to a request to access a user profile stored at a vehicle to determine whether the request is authorized, claims 7 and 17 further recite verification techniques, and claims 8 and 18 further recite authentication techniques. But Singh never describes *receiving a request to access a user profile*—and therefore never discloses performing any verification or authentication *in response to such a request* to authorize access to the profile. Ex. 2022 ¶¶ 280–288, 298–299; Ex. 1008 at ¶¶ 38-41. Nor does Petitioner identify any disclosure in Cazanas or Forstall that supplies this missing “request-to-access” trigger and the corresponding authorization gate for accessing a vehicle-stored profile. Ex. 2022 ¶¶ 302, 321–324.

Instead, Petitioner cites what it characterizes as redundant teachings with Singh and asserts that a POSA could apply them to “beneficially increase security,” without explaining what specific modifications to Singh a POSITA would be motivated to make. That is impermissible hindsight reconstruction, not an articulated, claim-mapped rationale for obviousness. Ex. 2022 ¶¶ 322–323. For this additional reason, Petitioner fails to demonstrate the obviousness of claims 6-8 and 16-18. Ex. 2022 ¶¶ 321–324.

X. GROUND 7: THE SINGH–ROVIK COMBINATION FAILS TO ESTABLISH OBVIOUSNESS OF CLAIMS 9–10 AND 19–20.

Petitioner’s arguments for claims 9-10 and 19-20 in Ground 7 depend solely on alleged teachings from Rovik (in combination with Singh). Petitioner’s arguments for Ground 7 fail for the same reasons as its arguments in Ground 4. Ex. 2022 ¶¶ 325-330. Petitioner relies on the same general motivation to combine for both grounds. *Compare* Pet. at 73-76 *with* 99-101. And Petitioner relies on the same alleged teachings of Rovik in both grounds, which suffer from the same misunderstanding of Rovik explained for Ground 4. *Compare* Pet. at 76-81 *with* 102-106.

As explained in Ground 4, Rovik does not disclose or suggest a vehicle-resident user profile based on a template, does not disclose creating an updated user profile relative to such a template, and teaches a fundamentally different, server-

centered architecture that a POSITA would not have been motivated to import into either Hendry or Singh. Ex. 2022 ¶ 330.

XI. CONCLUSION

The challenged claims should be upheld.

Date: January 9, 2026

Respectfully submitted,
AVANTECH LAW, LLP
80 S 8th St, Suite 900
Minneapolis, MN 55402
(855) 750-9951

/Eric A. Zelepugas/
Eric A. Zelepugas
Registration No. 73,302
Lead Counsel for Patent Owner

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

I certify that this paper complies with the type-volume limitations of 37 C.F.R. §42.24(B)(1) because it contains 18,432 words (determined by the word-processing system used to prepare this paper), excluding the parts of the paper exempted by 37 C.F.R. §42.24(a).

Date: January 9, 2026

Respectfully submitted,

/Eric A. Zelepugas/

Eric A. Zelepugas

Registration No. 73,302

Lead Counsel for Patent Owner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S RESPONSE** and associated exhibits (Exhibits 2021-2023) were served electronically via e-mail on January 9, 2026, in their entireties on the following counsel of record for Petitioner:

Patrick Colsher (Lead Counsel)
Matthew G. Berkowitz (Backup Counsel)
Reichman Jorgensen Lehman & Feldberg LLP
pcolsher@reichmanjorgensen.com
mberkowitz@reichmanjorgensen.com
rj_toyota-autoconnect@reichmanjorgensen.com

Date: January 9, 2026

Respectfully submitted,
AVANTECH LAW, LLP
80 S 8th St, Suite 900
Minneapolis, MN 55402
(855) 750-9951

/Eric A. Zelepugas/
Eric A. Zelepugas
Registration No. 73,302
Lead Counsel for Patent Owner