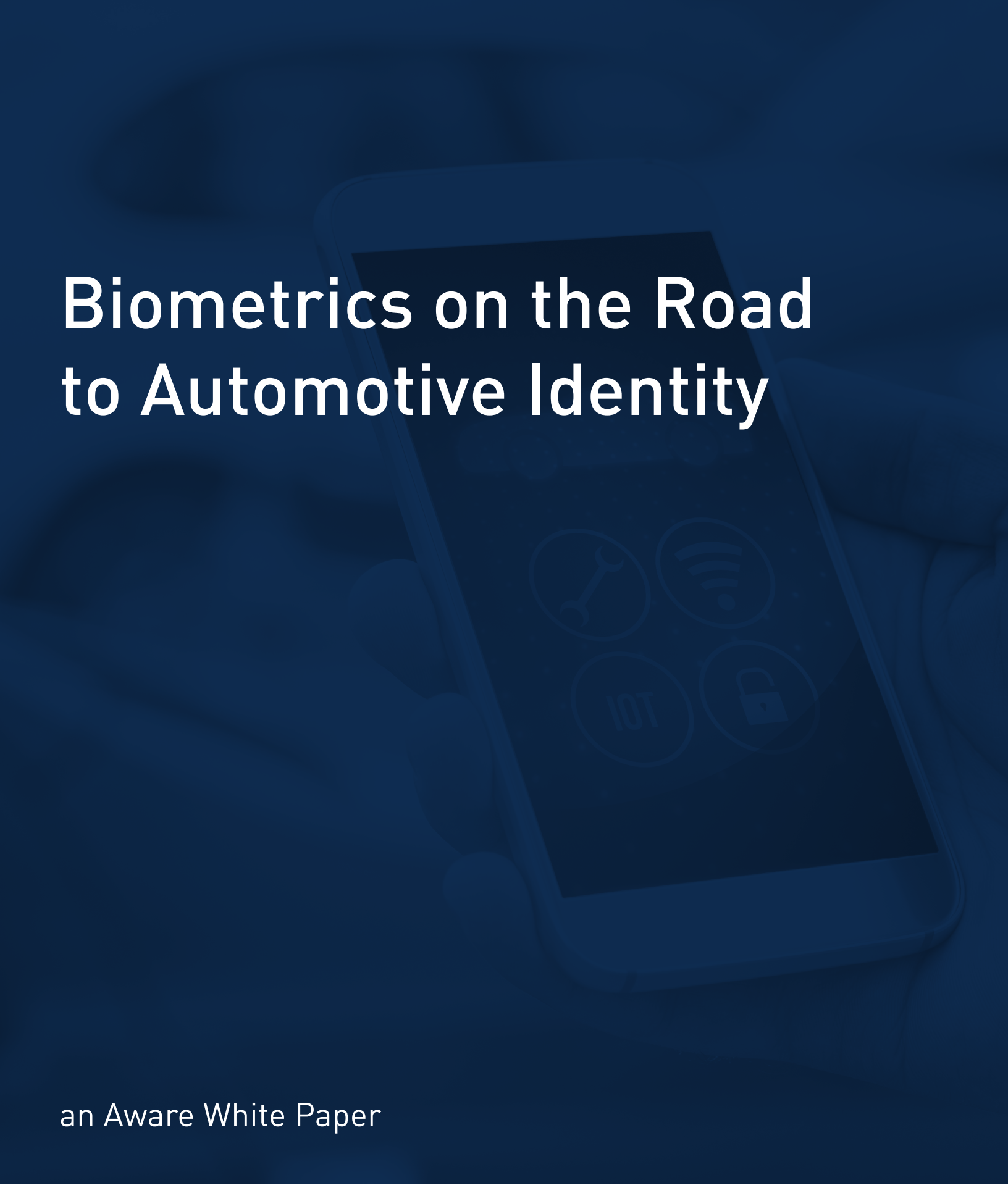

Biometrics on the Road to Automotive Identity

an Aware White Paper

AWARE

Part One:
The Connected Car Future

This is not your father's Oldsmobile. After a hundred years of incremental improvements in the performance, efficiency, safety, and reliability of our automobiles, today we are in the midst of what can be argued is a truly revolutionary change in what it means to drive a car. Our vehicles have become supercomputers on wheels, with hundreds of sensors collecting every imaginable datapoint, thousands of times every second. Advances in wireless connectivity such as those promised by 5G networks are transforming the way we hit the road. Vehicles of all types are connecting to the Internet and to each other, to the point where getting behind the wheel has turned from a convenient way to get from A to B into a highly personalized and efficient mode of transportation, that also happens to be safer than ever. But as connected cars and trucks take to our highways, it's not enough that they can navigate, connect, communicate, and entertain – this new wave of automotive transportation has to be personal. The smart vehicle of tomorrow needs to know its driver.

The automotive landscape is changing quickly. Innovative leaps in sensors, computer processing, artificial intelligence, and user interfaces have enabled new ways for drivers and passengers to interact with vehicles, and that has led to a mini-renaissance in transportation accessibility. Ridesharing services like Uber and Lyft turned every car into a potential taxi, car sharing companies like Zipcar turned every licensed driver into a partial vehicle owner, and pioneering automotive manufacturers like Tesla are changing the concept of driving altogether, with initiatives for AI-assisted driving, autopilot features, and even driverless vehicles.

New vehicular paradigms are the result of a massive convergence of high technology: mobility, IoT, and machine learning. The car has become a connected "thing" in the IoT, and one with signifi-

Identity is What You Are

Passwords and PINs are ineffective security measures because they can be lost, stolen, forgotten and cracked. Tokens and keys can be copied and fall into the wrong hands, too. In today's digital mobile world, the only way to irrefutably prove you are who you say you are is with biometric authentication. While this idea is gaining traction on the Internet and in mobile finance scenarios, it holds true in the physical world too. The connected car needs security based on the strongest level of identity technology, and that's why biometrics are hitting the road.

cant market appeal. Allied Market Research, in the report **"Global Connected Car Market,"** predicts the sector will grow from an estimated $63 Million in 2017 to $225 Million in 2025. The car is going online at a CAGR of 17.1 percent.

This conceptual shift opens new challenges when it comes to vehicle operation, cybersecurity, and road safety – in addition to the risks associated with driving, connected cars are also subject to the pitfalls of modern digital life. But vehicles aren't like a web browser or banking app; they are unique machines, at once highly ergonomic and necessarily designed for an optimal user experience. Drivers love their cars. Vehicles are major investments for the average motorist, and driving is a deeply personal experience.

That's why it's important that, as vehicles continue to go online and act as connected smart devices, strong identity technologies for authentication, identification and trusted interface are included in the greater transportation upgrade. In its report, AMR identifies hacking as a major threat to the connected car market, pointing to vehicle ecosystem, malware and backend dealer web portals as particularly vulnerable. Thankfully, there is a known solution to this challenge: strong identity enabled by biometrics.

With the integration of biometrics and other human interface technologies, connected vehicles ensure drivers remain at the center of the next phase of automotive evolution. Providing intuitive access control and safe remote start-up, driver ID, in-car payments, hands-free features, automatic preset adjustments and myriad passenger safety benefits, a smart car with strong identity tech is the only way to truly achieve the potential of connected automobiles.

Part Two: **When Vehicles Know Their Drivers**

The Key to Identity

The most familiar entrypoint to identity in the connected vehicle is the car key. Physical keys and remote locking fobs are the established means of access control for the personal vehicle. But as we've seen throughout the digital space in the past decade, with its record-setting data breaches and demand for convenient and strong authentication, 'something you have' is not enough when it comes to protecting connected assets. Through loss, theft, or duplication, something you have can quickly become something another person has, and that poses a problem when it's the keys to your car.

When a car is connected, however, the key becomes even more compromised as an identifier, with real life examples already existing of connected cars being hijacked remotely via bluetooth connection, giving hackers access to door locks, the parking brake, and even the ignition of vehicles, and posing serious threats to vehicles and their drivers. With keys that can be circumvented through wireless hack attacks, it's time for human presence to take the wheel.

Biometrics for car access outside the vehicle can be implemented through mobile apps or on-car sensors, but the effect is the same: biometric recognition ensures a live, authorized human being is unlocking doors and starting the car, not malware, or an unrecognized bad actor. And that's all before you even buckle your seatbelt.

Inside the car, built in sensors can identify and authenticate drivers and passengers alike. Face, iris, voice and fingerprint biometrics have all been integrated into automobiles for safety, security and comfort.

Sharing the Road

The emerging landscape of car sharing poses an interesting access control challenge, and connected car biometrics can help. Borrowing cars on a short-term basis through startup models offered by companies like ZipCar and Car-2Go means every car share customer needs to have limited access to a specific car for a specific window of time. Traditionally, contactless key cards and mobile apps have played the role of providing identity and access management, but a membership card doesn't prove who you are, just what you have. That poses a liability in the event of unlicensed drivers, collisions, and even car theft. Biometrics make car sharing natural.

The personal biometric vehicle

In addition to providing secure access and ignition controls, biometrics allow a vehicle to know who you are. This enables high levels of customization in terms of driver settings. Seat, mirrors and steering wheel adjustments, radio and streaming audio settings, linked payment accounts for toll and fuel transactions, and more can all be adjusted automatically with zero friction with passive biometric driver identification.

A connected car with built-in facial recognition, for instance, can authenticate a driver profile when they sit down and switch to a favourite playlist, while an unauthorized user rejected by the face scan might have limited or no access to any car functions. The biometrically authorized driver could pay for fuel using biometrically-bolstered hands free voice controls, and an identified driver can potentially lower his or her insurance premiums thanks to verified safe driving. Even vital biometrics in car seats and seatbelts have a role to play when it comes to vehicular safety, such as through the measurement of heart rates to detect driver alertness and health.

While the technology described here may sound futuristic, it is all available for integration today. But with such powerful connected technology comes the need for responsible best practices. Deploying biometrics on connected vehicles demands certain key considerations:

Liveness detection

Biometrics advance both security and convenience, but where security is the dominant motivation, liveness detection is critical for both face and voice modalities. For some uses of automotive biometrics, there can be motivation to "spoof" the biometric matching process with a fake reproduction, such as a photo, digital image, or voice recording of the targeted identity theft victim. Liveness detection technology is used to ensure that facial images and voice samples are real and live.

Identity Proofing

Not just anyone can drive a car. You need a valid license and insurance. It is therefore critical that biometric access in the connected car starts with a strong foundation of trust. Upon

The Car on the Edge

Personal vehicles pose an interesting proposition in terms of biometric storage and matching. Multiple authorized drivers necesitate a 1:few matching, which means each car will need to store multiple biometric templates, each associated with a unique user profile. Furthermore, authentication must be possible in network dead zones. These considerations suggest a novel biometric matching paradigm is required in which matching of different individuals can be performed on device (in the car).

mobile biometric enrollment and verification of a driver's license, it is integral that the biometric templates used to identify the driver are bound to the right person. Liveness detection is again an imperative to ensure that the onboarding process is secure. An identity-forward connected car needs to be 100 percent sure who is driving.

Optimal modalities

As ubiquitous as it is, driving is a high-risk action, so in-vehicle biometrics must be deployed with an eye for safety. Hands-free modalities like face and voice work best for making sure drivers stay focused on the road while staying authenticated.

Data storage and privacy

Adoption of automotive biometrics is critical for the connected car, but car owners need to be comfortable with the security and privacy of their personal and biometric data. Biometrics are not secrets, they are privacy-enhancing by design, but they must be deployed through a consent-based framework that empowers the user and is flexible enough to make sure no one is locked out and stranded on the side of the road.

Thankfully, the maturity of biometrics in enterprise, financial services and government sectors has paved the way for everyone from the automotive manufacturer to the vehicle-based startup to make responsible and ethical choices when bringing biometrics to the streets.

Part Three: **Commercial Use Cases of Biometric Vehicles**

Vehicles are more than just personal transportation; they serve as the foundation of many commercial industries and public services. Just as the personal automobile has transformed with the advent of mobility, AI, and connectivity, so too have the myriad vehicle-based businesses, old and emerging. Identity, based on the trusted foundation of biometrics, is necessary all over the road.

Here are just some of the commercial use cases for biometric automotive identity outside and inside the car:

COMMERCIAL USE CASES	OUTSIDE CAR	INSIDE CAR
Car Sharing	Car sharing services like ZipCar and Car2Go need to provide their massive user base limited-time access to large scale vehicle networks. A biometrically enabled mobile app can provide the necessary trust and security to act as a temporary key. Once a car is claimed by the user, a digital credential can be issued to the driver's device, which, with biometric authentication, can open doors and even offer remote start.	Car sharing scenarios are the perfect use case for biometric custom presets. A driver profile with entertainment and in-car environment presets activated through a biometric scan brings the bespoke experience previously exclusive to car ownership to the car sharing experience. With biometrics, every car can feel like your car.
Transportation Networks and Taxi Services	Taxi services and transportation networks like Uber and Lyft can add a layer of trust to user profiles. Biometrics ensure each customer profile can only be used by the real enrolled user. That means two things: users say goodbye to stolen and hacked accounts and networks know their customers are who they say they are, increasing accountability and safety.	In the car, biometrics turn the transportation network into a well functioning remote workplace. Drivers can biometrically log hours while networks and taxi companies can ensure only authorized, licensed drivers are taking fares.

COMMERCIAL USE CASES	OUTSIDE CAR	INSIDE CAR
Vehicle Rental	Similar to car sharing, rental services can use biometrics to issue temporary mobile keys for vehicle access and remote start. Registration and payment can be made easy too, since biometrics can be used as a trusted link between a driver, their license, and insurance information. This allows for automated rental and new remote customer service experiences.	In addition to the biometric preset customization in the "Car Sharing" section above, biometrics can be used to enable in-car payments, allowing rental services to offer in-car value added services like access to satellite radio, premium passenger entertainment, and in-car Internet access.
Bussing	Biometrics on the bus can make sure no traveller is left behind at rest stops on long haul routes and school field trips. Deployed with consent-based best practices, a face scan upon boarding is an easy and frictionless way to ensure everyone's on board before the wheels start turning.	On the bus, biometrics can track driver attendance, too, while also ensuring the chauffeur is alert, awake and driving safe. New computer vision technologies can assess a driver's alertness, ensuring proper measures are taken in the event they become fatigued. The biometric bus is a safe bus.
Delivery	Biometric ID can track mail from point A to point B, with an unimpeachable audit trail. Upon arrival, given the proper identity infrastructure, a recipient's biometric can verify delivery with greater assurance than the traditional signature.	Biometrics help delivery companies understand the schedules and activities of their drivers. This data can be used to optimize routes and to compensate drivers for extra hours.
Trucking	When biometric ID is associated with licensing data, a truck can stay locked to all but those with the demonstrated know-how. Furthermore: the ability to integrate special credentials into a connected vehicle ID ecosystem can make transporting sensitive cargo more efficient and trustworthy.	Existing fleet management software, which leverages telematics and wireless tech to track drivers, can offer more actionable analytics when associated to a biometric identity. This can help encourage safe driving habits through personal incentives. Managers can know with confidence not just where vehicles are but where drivers are.

Revving up in the Era of Remote and Mobile Work

For many workers in the contract and gig economy, the connected car is tantamount to the modern office. As such, biometric solutions pertinent to the modern enterprise cross over significantly with commercial vehicular identity applications. Learn more about biometrics and the contemporary business landscape by reading Aware's recent white paper: **Enterprise Security in the Age of Remote and Mobile Work**.

Part Four: **Beyond Convenience and Security**

In addition to the convenience and security benefits that identity awareness deliver, the biometrics-enabled vehicle also offers an environment where related technologies are able to increase safety. Namely: eye tracking, speech recognition, and expression detection.

The new role of voice in the car

Perhaps the most familiar in-car recognition technology is hands free voice control enabled by speech recognition. This safety feature enables the responsible use of GPS, communications, and entertainment interfaces. You can keep your hands at 10 and 2 while re-routing in car navigation to the next gas station. You can take that important work call without touching your phone and endangering yourself, your passengers, or other drivers. You can change your music playlist, check weather forecasts, and get traffic reports just by speaking to your car.

Alone, speech recognition is a convenient safety feature, enabling the always-connected lifestyle without compromising the safety of those on the road. But coupled with biometric authentication technologies, the potential for hands free controls expands dramatically. Biometric authentication can identify speakers, ensuring the driver is in control of in-car audio. It can also enable contactless conversational commerce – allowing you to order ahead for coffee at a rest stop, or authorize a payment to a gas station with a simple phrase.

The new role of face in the car

Computer vision technology in the driver's seat has the potential to save lives. In addition to providing the biometric data for authentication, other measurements in a driver's visage can be observed relating to awareness, fatigue and general performance. Face recognition and eye-tracking can monitor a driver's face to see if they are too tired to drive or nodding off, enabling the activation of secondary safety measures. It can potentially be used to detect drunk drivers, preventing ignition before inebriated drivers have the chance to do damage.

And it doesn't just have to be safety prevention, either. Computer vision can be deployed as part of a driver monitoring service for insurance companies, rewarding drivers who consistently check blind spots with reduced premiums.

Together with biometric identity and authentication technologies, speech recognition and AI-empowered computer vision help your car learn who you are and how you drive.

Part Five: **Get in the Car**

The Identity Empowered Automotive Landscape is on the Horizon

Connected cars are not science fiction. They are a key part of the IoT future where user experience is as crucial as identity-based physical and information security. Auto manufacturers, vehicle-dependent enterprises, and average car owners the world over need to trust in biometrics so that all of us can trust the roads of the future.

Aware, Inc. provides the biometric software, products and services that can put strong identity in the driver's seat. With multi-modal biometric flexibility and world-leading expertise in identity proofing, mobile authentication, and high-performance matching liveness detection both on-device and on-server, Aware is ready to put people back at the center of the automotive industry.

For more information, visit **Aware.com** today.

About Aware, Inc.

Aware is a leading global provider of biometrics software products and solutions used to collect, manage, process, and match biometric images and data for identification and authentication.

Our products include complete biometric software solutions as well as the modular components used to build them: SDKs and applications for enrollment; fingerprint, face, iris, and voice matching algorithms; mobile biometric capture and authentication software; a biometric workflow and middleware platform, and a biometrics-as-a-service platform.

These products fulfill critical biometric functionality for applications in financial services, enterprise security, healthcare, human resources, citizen ID, border management, law enforcement, defense, and intelligence. Aware is a publicly-held company (NASDAQ: AWRE) based in Bedford, Massachusetts.