Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Autonomous vehicles

"It's all about you!"
The integration of biometrics into autonomous vehicles

NORTON ROSE FULBRIGHT

Norton Rose Fulbright: Where can we take you today?

Paul Keller
Partner, New York
Tel + 1 212 318 3212
paul.keller@nortonrosefulbright.com

Barbara Li
Partner, Beijing
Tel + 86 10 6535 3130
barbara.li@nortonrosefulbright.com

Frank Henkel
Partner, Munich
Tel + 49 89 212148 456
frank.henkel@nortonrosefulbright.com

More than 50 locations, including Houston, New York, London, Toronto, Hong Kong, Singapore, Sydney, Johannesburg and Dubai.

Attorney advertising

Autonomous vehicles

“It’s all about you!”
The integration of biometrics into autonomous vehicles

Contents

I. Introduction

Norton Rose Fulbright's fourth annual Autonomous Vehicle (AV) White Paper addresses the planned and actual use of biometrics – the measurement of unique human physiological and behavioral characteristics – in today's (and tomorrow's) vehicles. To be sure, the use of biometrics has been incorporated into a multitude of technologies that are used on a daily basis to facilitate the identification or authentication of individuals. Such technologies have long included the use of fingerprint and facial recognition to unlock laptops and cellphones and for identification at border crossings, and voice recognition to verify identity for financial transactions. Now the technology is being pushed to include hand gesture recognition (e.g. swipe gestures), gait recognition, and facial and hand thermograms, all of which may be used by companies for marketing and by governments to conduct surveillance.

The automotive industry is increasingly incorporating biometric technologies for both security and convenience into their vehicles, especially for the next generation of AVs. With this rapid embrace of biometrics comes significant concerns relating to protecting the privacy of individuals. Only a few states have passed laws regulating the collection and security of biometric data. Uniformity of regulations, however, is lacking. These biometric innovations also have been developed at great cost to companies both inside and outside of the rapidly changing car industry. Although each developer believes that their particular technologies should be embraced by its marketplace, the field continues to evolve, and customer preferences are still very much undefined. Companies, therefore, have sought and continue to seek to protect their innovations through the panoply of intellectual property rights, most specifically patent rights, that will allow them to preclude unauthorized users from taking their hard-earned market share.

This White Paper explores the legal issues raised by the increased use of biometrics in cars and how to manage the risk that they raise for vehicle developers, manufacturers, and operators. As a starting point, the basic contours of the different biometric technologies are discussed. With that understanding in hand, this White Paper explores the laws of eight countries and their impact on biometric use. The countries discussed include:

- United States
- Australia
- China
- France
- Germany
- Indonesia
- South Korea
- Turkey

II. The integration of biometrics into autonomous vehicles

A. Biometrics technological overview

Although the topic of "biometrics" can be addressed in a number of ways, there are two fundamental points – the types or "what" information can be used, and the method or "how" that information is captured. Far beyond merely capturing an ink impression of an index finger or a partial of a thumb, today's biomarkers cover a wide range of the human condition and are captured and stored in a myriad of ways that provide both great benefits and significant challenges. These are discussed below.

Biometric characteristics, the "whats," are separated into two modalities, physiological and behavioral.[1] Physiological characteristics include those identified from the fingers and hands, veins, face, eyes, ears, odor, and DNA. In contrast to physiological traits, behavioral characteristics (or a combination of both physiological and behavioral traits) also are increasingly utilized by biometric systems. Behavioral characteristics are generally dynamic and can be affected by various factors, including age, illness, or emotional state.

(i) Hands

Fingerprints – Fingerprint recognition is one of the most well-known applications of biometrics. It is a commonly used physiological biometric for US Customs and Border Protection to control international border entry points.[2] It is also an integrated authentication feature in most cellphones on the market today. Fingerprint recognition involves recognizing the unique differences in patterns of certain characteristics of fingerprints, such as whorls, ridge patterns, and minutiae points (the points plotted to ridge endings and ridge discontinuities) which differentiate the fingerprints of different individuals.

Fingerprints are first acquired and imaged by either off-line or online techniques. Off-line techniques first require that the fingerprint be captured on a substrate, such as inked fingerprint on paper, and then digitized. Online acquisition, such as a live scan of the fingerprint with optical or capacitive digital imaging technologies, would directly create a digital image.

Most scanners, however, do not scan the entire finger at once and also do not create a full image from all the partial images.[3] Using software algorithms, the features of the fingerprint (e.g. ridge orientation and frequency, ridges, and minutiae) are extracted and a biometric template is created. This template is a sequence of binary data that can be used to compare another sequence acquired from a subject for identity or authentication purposes. These templates may be either proprietary templates that are coded to distinct fingerprint recognition systems or standard templates that are interoperable between vendors. In order to achieve interoperability between competing fingerprint recognition systems, an initiative led by the US Department of Commerce's National Institute of Standards and Technology (NIST) created standards for fingerprint recognition.[4] Depending on the purpose for which the fingerprints are acquired, the biometric data may be stored locally on the device or on a secure portable smart card (e.g. for mobile banking) or on a server (e.g. for government identification purposes).

Palm & hand – Palm recognition also utilizes physiological measurements similar to those used in fingerprint recognition (e.g. matching minutiae points and ridge patterns).[5] Some law enforcement agencies, including those in Connecticut, Rhode Island, and California, have established palm print databases to identify potential criminal offenders.[6] Interestingly, at a recent security conference, researchers from NYU were able to create artificial fingerprints that contained some features of

1 For a more in-depth review of biometric modalities discussed herein, *see* Traore et al., *State of the Art and Perspectives on Traditional and Emerging Biometrics: A Survey*, e44 Security & Privacy 1 (Oct. 16, 2018) (https://doi.org/10.1002/spy2.44); Anil K. Jain et al., Introduction to Biometrics (2011); FBI, Biometric Center of Excellence (BCOE) – Modalities, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/modalities (last visited Nov. 13, 2018).

2 Marcy Mason, Biometric Breakthrough: How CBP is Meeting Its Mandate and Keeping America Safe, US Customs and Border Control, https://www.cbp.gov/frontline/cbp-biometric-testing (last visited Nov. 13, 2018).

3 Alex Hern, *Fake Fingerprints can Imitate Real Ones in Biometric Systems – Research*, The Guardian (Nov. 15, 2018), https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research.

4 *See* NIST, INCITS Standardized Biometric Data (Dec. 10, 2016), https://www.nist.gov/itl/iad/image-group/resources/incits-standardized-biometric-data; Danny Thakkar, Interoperability Guidelines in Biometric Fingerprinting, Bayometric, https://www.bayometric.com/interoperability-guidelines-in-biometric-fingerprinting/ (last visited Nov. 13, 2018).

5 FBI, Palm Print Recognition, https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-palm-print-recognition.pdf (last visited Nov. 13, 2018).

6 *Id*. at 122.

fingerprints that were more common than others.[7] The artificial fingerprints were able to fool the fingerprint sensor more than one in five times. These manufactured fingerprints were designed to target fingerprint scanners like those in cellphones.

Another related physiological biometric is hand geometry. Hand geometry recognition is the longest implemented biometric type. Commercially available systems for measuring hand geometry have been available since the early 1970s.[8] Hand scanners were used in the 1996 Olympic Games to control access to the Olympic Village.[9] It can involve the measurement of the length, width, thickness, and surface area of the hand, as well as the distance between knuckles, and the height or thickness of fingers. However, unlike fingerprints, hand geometry is not as unique and an individual's hand geometry may change over time.

Both palm prints and hand geometry can be captured as high or low resolution images from charge-coupled cameras, digital scanners, webcams, contactless systems, and thermal, among others. As with fingerprint technology, the palm has certain identifying features, including ridges, valleys, and minutiae, that can be used to generate a biometric template. One advantage palm prints have over fingerprints is that the palm is larger, and thus has more information to use to create the biometric template. The captured images are preprocessed to smooth the image and enhance contrast. Depending on the system, a variety of algorithms can be used to extract features from an identified region of interest on the palm and create a biometric template. For hand geometry, the image of the hand is processed by an algorithm and converted to a numerical representation, which is then stored as the user's biometric template. These biometric templates are stored in a database that can reside on the device's memory, an identification smart card, or on a server.

Veins & face/hand temperature – Vein patterns in the hands or fingers are another biometric characteristic that can be used to authenticate identity. Financial institutions have utilized vein pattern biometrics in ATMs and for customers accessing safe deposit boxes.[10] Vascular patterns are captured through the use of near-infrared light, which is readily absorbed by the deoxygenated blood carried by veins and renders the vein patterns visible. An additional benefit to vein pattern biometrics is that the vein pattern is stable over an individual's lifetime and, unlike fingerprint or hand geometry recognition, can only be used to authenticate a living individual. Another related biometric technology uses infrared thermograms that recognize the pattern of heat radiation from the face or hand. Thermograms are unique to an individual since the thermal patterns are derived from the vascular structure of the individual. Thermograms can serve to not only identify or authenticate identity but to also verify that the biometric measurements are from that of a living individual.

Infrared and near infrared imaging is used to capture the unique patterns of heat that the individual radiates from their blood vessels in their face, hands, and the veins of his or her hands. This is a non-intrusive and non-invasive technology. This imaging of heat is then converted into a temperature, and the patterns are encrypted and stored in a similar manner as with templates previously discussed above.

(ii) Head

Face & ear – Biometric facial recognition is another technology widely used for authentication and identification purposes. Facial recognition technology is used worldwide by law enforcement agencies, including at least two separate FBI programs[11] and with social media platforms like Facebook. Facial attributes are captured by photometric or geometric sensors. The geometric method analyzes the shape and position of facial features (e.g. the distance between the eyes, cheekbones, chin, and nose) and relies upon distinguishing facial features. The photometric method converts the facial features into numerical values, creating a template based on the values, and then compares that template to the values for facial features from another image for identification or authentication purposes. Similarly, ear recognition is used in biometric technology because the shape of the ear is stable over time and its growth is almost linear with aging. As with facial recognition, ear recognition can be assessed based on matching distances between structural points in the ear or by matching based on the appearance of the ear.

7 Hern
8 Jain et al. at 186.
9 Duta et al. at 2803.
10 Patrick Collinson, *Forget Fingerprints – Banks are Starting to Use Vein Patterns for ATMs*, The Guardian (May 14, 2014), https://www.theguardian.com/money/2014/may/14/fingerprints-vein-pattern-scan-atm.
11 See Kimberly J. Del Greco, Statement Before the House Committee on Oversight and Government Reform – Law Enforcement's Use of Facial Recognition Technology, https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology

Sensors are used to capture facial or ear features. These distinguishing facial features are analyzed with respect to their size or relative position to other facial features. The shape of the face is also an important feature. The spectral band of the sensor can be visible, infrared or thermal, and the image may be rendered as a 2D photograph, 3D image, or video. Different algorithms create a biometric template based on these distinctive features for later authentication use. In order to facilitate interoperability, NIST has also propagated voluntary consensus standards for the interchange of facial biometric data.[12] Similarly, ear recognition utilizes algorithms which extract distinctive features based on the shape of the ear and converts the images to a numerical format, which is incorporated into the individual's biometric template.

Eye – The eye is also the source of multiple traits used in biometric systems. Iris recognition systems have been used in universities for access to on-campus dining halls and, recently, plans have been announced for facial and iris recognition for check-in and boarding purposes at the Dubai International Airport.[13] The iris of the eye, the colored ring around the pupil, is considered the most accurate of biometric traits. The iris is also unique, even between the left and right eyes of the same individual, and there are many distinguishing features present in the iris (e.g. striations, rings, furrows, freckles; but generally not color) that can be utilized in an iris recognition system. The retina is another reliable and accurate trait of the eye that is used in biometric systems. The US military utilizes laptop computers and handheld identity detection equipment with retinal scanners in Iraq and Afghanistan to identify local suspects.[14] The retinal vasculature is also considered a distinctive feature between individuals that is difficult to replicate. Similar to vein recognition, the eye is scanned with infrared light and the unique retinal vasculature is compiled into a template for the biometric system. However, due to the difficulties in image acquisition, the use of eye traits in biometric systems is not as well-adopted as fingerprint or facial recognition has been.

Although both the iris and the retina are essential parts of the eye, biometric data is gathered differently for the two. The iris is scanned with near infrared cameras to identify the distinctive textural details present in the iris. An algorithm converts the complex pattern in the iris into digital data that is stored in a database as a biometric template or used to compare against a stored template. In contrast to the iris, it is the vasculature of the retina that is of interest. In order to image the retina's vasculature, visible light is beamed into the eye, where the retinal blood vessels absorb it. The amount of light reflected back changes as a result of the vasculature in the retina. These changes in the light pattern during the scan are then converted into code and stored in a database.

(iii) Intrinsic factors

Body odor – As with bloodhounds, body odor recognition relies upon identifying the unique chemical patterns of an individual's scent.[15] Every individual exudes an odor that is characteristic of its own chemical composition. These patterns of chemical composition are thought to be unaffected by the use of deodorant, diet or disease, and the detection methods are less intrusive than with biometric recognition systems involving the eye or fingerprints.

The characterization of an individual's body odor is done by analyzing the air in the environment around the individual. A sensor reacts with the organic substances in the air and a chromatogram identifies the odor's composition. The composition is then converted to digital format and stored in a database.

DNA – DNA patterns are distinct between individuals and, as such, DNA is a useful biometric modality for identification and authentication systems. However, the utility of DNA recognition in biometric systems outside of forensics is limited due to the lack of real-time recognition capabilities and the ease of sample contamination.

DNA identification involves measuring the lengths of short tandem repeat (STR) sequences present in the nuclear or mitochondrial DNA. The number of repeated DNA sequences in these STRs differs greatly between individuals. DNA is also inherently digital, and thus does not require an additional step to convert its data into another a template. However, the time required to complete a DNA analysis is prohibitively long for use in mass identification or authentication (e.g. border crossings). Care must be taken to not cross-contaminate the samples with another individual's DNA.

12 Charles H. Romine, Facial Recognition Technology (FRT), NIST (Mar. 22, 2017), https://www.nist.gov/speech-testimony/facial-recognition-technology-frt.

13 See Raquel N. DeSouza, *Optic Technology Grants Access to Anytime Dining*, Fourth Estate (Aug. 27, 2014), http://gmufourthestate.com/2014/08/27/optic-technology-grants-access-to-anytime-dining; Cleofe Maceda, *Emirates to Introduce Facial, Iris Recognition Technology to Flyers*, Gulf News (Oct. 29, 2018), https://gulfnews.com/business/aviation/emirates-to-introduce-facial-iris-recognition-technology-to-flyers-1.2295248.

14 US Army Corps of Engineers, Introduction to Biometrics and Biometric Systems (Feb. 3, 2013), https://www.tam.usace.army.mil/Portals/53/docs/UDC/Biometrics%20101.pdf

15 See P. Inbavalli and G. Nandhini, *Body Odor as a Biometric Authentication*, 5 Int'l Journal of Comput. Sci and Info. Techs. 6270–6274 (2014).

(iv) Movement

Gait – The pattern of human locomotion, or gait, can be used for biometric systems based on behavioral characteristics. Algorithms are used to extract an individual's gait features, both dynamic and static (such as body shape). Although gait recognition can be obtained non-intrusively, an individual's gait can be altered by many outside factors (e.g. walking surface, footwear, clothing) or can change with age or weight variations.

Gait analysis can be performed with low-quality video footage of a person walking. In some instances, many cameras are placed all around the individual to capture all angles of a person's gait. Sensors can also be placed on the floor to measure unique footstep patterns. The video footage can then be used to generate a blurred silhouette, which can also be used as the biometric template. Gait analysis involves not only dynamic gait motion but also static body appearance. Given that a person's gait can be affected by a myriad of external issues (e.g. footwear, walking surface, etc.), there is a question as to how unique an individual's gait actually is.

Signature – Another behavioral biometric is the way an individual signs their name. Signature recognition involves the measurement of the dynamic movements that an individual demonstrates as they sign their name. Such dynamic characteristics are difficult to mimic and include the direction of movement, the pressure exerted, stroke order and direction, speed and shape of the signature. However, an individual may have large variabilities in these dynamic movements between signatures, and signature recognition may be difficult.

The dynamic act of signing a signature can be measured and analyzed to isolate the unique dynamic movements used during the signing. Alternatively, the individual could provide a static sample signature, which is then turned into a digital image and analyzed by a software algorithm. Dynamic signature recognition is extremely difficult to replicate because the forger would have to physically copy the signer's dynamic characteristics (e.g. acceleration, timing, pressure, etc.).

Keystroke – The behavioral biometric of keystroke rhythms is considered sufficiently distinct between individuals to use for identity verification purposes. Keystroke dynamics involve the manner and rhythm of an individual's typing on a keyboard. An individual's keyboard dynamic measurements may not be unique, but keystroke software can capture data based on the typing pattern, rhythm, strength and speed. Additional biometric parameters include the duration that a key is pressed, the dwell time, and the duration between releasing a key and pressing on the next key, flight time. These parameters are all utilized to generate a biometric template. Keystroke dynamics can, however, be affected by physical issues affecting the hands or muscles, emotional state, and the keyboard used. Monitoring of keystroke dynamics over the course of a session also allows for continuous verification of the individual's identity. The Bank of Utah also incorporated keystroke dynamics software to enhance the security of its online banking platform.[16] While keystroke dynamics are non-invasive and require no additional hardware, typing patterns are not as consistent as some believe. MIT found that keystroke patterns were affected by a change in the keyboard used, the keyboard layout, and physical discomfort in the hands.[17]

Gesture – More recently, gesture-based recognition systems have also been considered for biometric identification or authentication. Gesture recognition has been called "the mathematical interpretation of a human motion by a computing device."[18] Generally, gesture recognition tracks the movements of the hand or the face, but can also include tracking the head and/or body movements. Gesture parameters measured include acceleration, pressure, size, and time. Gesture recognition has been embraced in home game consoles, such as the Wii, Xbox, and Playstation, which have controllers with accelerometers and gyroscopes and readily respond to gestures. These same gaming companies also make their own gesture recognition software. Yamaha also introduced a gesture recognition feature on a motorcycle; it turned the engine on and off with a gesture.[19] Algorithms used in gesture recognition software are 3D-based or appearance-based models. 3D-based models rely upon information gathered from the rest of the body.

16 Jeff Vance, Beyond Passwords: 5 New Ways to Authenticate Users, Network World (May 31, 2007), https://www.networkworld.com/article/2290245/lan-wan/beyond-passwords--5-new-ways-to-authenticate-users.html.
17 Lau et al., *Enhanced User Authentication Through Keystroke Biometrics*, Dec. 9, 2004, https://people.csail.mit.edu/edmond/projects/keystroke/keystroke-biometrics.pdf
18 *Id*.
19 Chris Burt, *Yamaha Demonstrates MOTORiD with Facial and Gesture Recognition*, Biometric Update, https://www.biometricupdate.com/201711/yamaha-demonstrates-motorid-with-facial-and-gesture-recognition (Nov. 14, 2017).

(v) Combinations

Voice – Voice recognition is a combination of both physiological and behavioral characteristics. An individual's voice results from the static physical aspects of the body that are responsible for generating sound, such as the mouth, jaw, larynx, throat, nasal cavity, or weight. The behavioral aspects may reflect factors including language, age, or physical or emotional state. Voice recognition technology is used by many financial services companies to authenticate their clients.[20] Unlike speech recognition, which only attempts to recognize sound waves based on samples of words spoken from a large variety of people of different characteristics and backgrounds (e.g. sex, age, race, geographic, etc.), voice recognition is used to authenticate an individual and requires a match between the voice of the individual and a unique digital template of that individual's voice. For example, the US previously used a 24-hour voice-activated US-Canada border crossing for registered local residents of Scobey, Montana.[21] These residents would pick up a telephone at the border gate, enter a preselected four-digit personal identification number (PIN), and utter a secret pass phrase, which had previously been recorded at the border post. Once authenticated by the voice recognition system, the driver could proceed across the border.

This digital template is a master voice print generated by voice recognition software that often requires the individual to repeat a phrase or series of numbers or words several times before the software will have enough data points to accept the voice print as a template. These spoken words are reduced to segments of tones (dominant frequencies) that are captured by the software, converted into a digital equivalent, and stored as a template. These tones digitally represent the individual's unique voice template. Other voice recognition software utilizes the voice patterns of the individual, instead of repetitive phrases, to create the master voice print. This generation of the master voice print can be affected by outside influences, such as unnatural speech, background noise, and poor microphones. Voice recognition can also be affected by an individual's condition (e.g. have a cold, be affected by medications, or mood). Another challenge with voice recognition is that software recognition may be fooled by a voice recording, but most systems have either incorporated some form of liveness detection or use a secondary input, such as a unique PIN.

20 Maria Lamagna, *Banks Want Your Voice to be Your New Password*, MarketWatch (Feb. 26, 2016), https://www.marketwatch.com/story/banks-want-your-voice-to-be-your-new-password-2016-02-25.
21 James Brooke, *Remote Border Crossing Tuning to Remote Control*, N.Y. Times (Jan. 2, 1996).

B. Biometrics – Data storage and use

With the embrace of biometrics by many different industries for identification and authentication purposes and the increasing presence of technology that can passively collect biometric data (e.g. facial recognition and gait), the storage and security of the captured biometric data is of paramount concern since the physical and behavioral characteristics that underlie the biometric data is generally unchangeable. Biometric data is typically encrypted and can be stored (1) locally in an individual's device (e.g. fingerprint in cell phone; biometric information stored on smart card), (2) on a centralized server that may reside inside or outside of the country, or (3) through a distributed data model, which can break the biometric data into separate files that are then stored in two or more locations (e.g. locally on a secure card or cell phone and on a server).[22]

In general, the underlying biometric modality is captured and then the biometric system applies an algorithm, which may be proprietary to the system, and converts the original biometric data (e.g. fingerprint, facial recognition, vein pattern, etc.) into a numeric representation that is then used as the biometric template for comparison purposes. In order to authenticate or identify their identity, the individual's biometric comparator is converted into a numeric template that is then compared to the original biometric template. These biometric templates are encrypted, and it is extremely unlikely that the biometric template could be used to reverse engineer the original biometric measured.

Local storage of encrypted biometric data can be compromised if the device or smart card is lost or stolen. Also, as even the US Office of Personnel Management learned, biometric data stored on a server can be vulnerable to a cybersecurity breach; over 5.6 million people's fingerprints were taken during the breach.[23] Of the three options noted above, the distributed data model is the most secure at protecting biometric data from data breaches since all the parts of the data are stored in multiple locations. Nevertheless, if the servers that store the data are located in a foreign jurisdiction, then foreign law may govern how the biometric data is protected. For example, in the US there is no federal law that governs the gathering and management of intellectual property data. In most US states, biometric data can be collected and shared by businesses. Illinois, Washington and Texas have all enacted specific

22 *See* Jain et al. at 259–302; John Weir, Biometrics 101 (part II): Storing and Matching Biometric Templates, SecureIDNews (Mar. 1, 2004),https://www.secureidnews.com/news-item/biometrics-101-part-ii-storing-and-matching-biometric-templates/.
23 Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, Washington Post (Sept. 23, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches.

biometric privacy laws, and several states have included biometric data into their data breach notification laws.[24] In contrast, in the European Union, member states are required under E.U. data privacy law, the General Data Protection Regulation, to prohibit biometric data from being shared with a third party without consent, subject to a few exceptions.[25]

C. Biometrics in the automotive industry

Many of these biometric technologies are being considered for incorporation into the next generation of automobiles to enhance safety, convenience, and customization of the driving experience. At the 2018 New York International Auto Show, Genesis, a Hyundai division, introduced the Essentia Concept car that incorporated fingerprint and facial recognition technology for vehicle entry.[26] Iris and voice recognition are also other biometric modalities that can be used for verification of identity for vehicle entry. The incorporation of biometric entry and biometric ignition systems would eliminate the need for keys and hackable key fobs and should further deter car theft.

Unfortunately, the incorporation of a fingerprint recognition system does not guarantee that the vehicle cannot be stolen. For example, car thieves in Malaysia in 2005 bypassed the fingerprint security measure by cutting off the end of the car owner's index finger and using it to start the car.[27] Third-party companies that sell aftermarket parts have also created biometric car starter kits that require a registered fingerprint before the vehicle will start.[28] Jaguar has proposed the use of a facial and gait recognition system to unlock the car doors upon detecting the approach of an authorized user. The use of gait recognition would also prevent unauthorized access of the vehicle with a static picture of an authorized user.[29]

Auto manufacturers are also integrating face and iris recognition technology with a vehicle camera system directed at the driver to detect fatigue or drowsiness. The car would sound an alert if fatigue or drowsiness is detected.[30] Moreover, if this technology is incorporated in an AV, the vehicle could take over operating the car once the driver shows signs of drowsiness.[31] Biometrics to monitor the health of the driver have also been proposed, including infrared technology and Doppler sensors that monitor the driver's facial temperature and heart rate.[32] In an AV, the car could pull over to the side of the road or be programmed to call emergency services for assistance if the driver shows signs of being ill.

Biometrics can also be utilized for vehicle in-cabin preferences and personalization for vehicles with more than one driver. For example, in-cabin iris scanning technology can authorize a driver to start the car and automatically adjust the seats and mirrors and load music and GPS locations to the driver's preset preferences.[33] The Jaguar facial and gait recognition system described above would also allow the automatic personalization of the vehicle functions and features upon recognition of an authorized user.[34]

Voice recognition technology is now a relatively common feature in automobiles. Voice recognition in vehicles enable to driver to perform tasks (e.g. controlling navigation and music and answering connected cellphone) without taking their eyes off the road. In 2012, only 37 percent of new cars included a voice recognition system.[35] For cars manufactured in 2019, 55 percent of the new cars are anticipated to have a voice recognition system installed. By 2022, nearly 90 percent of all new vehicles are predicted to have voice recognition systems.[36]

Gesture recognition is another biometric that the automotive industry is embracing for in-car controls.[37] A camera would be mounted on the steering wheel or dashboard to look for registered gestures that would then activate a processor to analyze the gesture commands and execute functions based on those gestures. The recognizable gestures would need to be performed within a defined space and would also be without

24 Biometric Data and the General Data Protection Regulation, Gemalto (Aug. 20, 2018), https://www.gemalto.com/govt/biometrics/biometric-data.
25 *Id*.
26 Press Release, Genesis Motors, Electrifying Escapism: Genesis Reveals Essentia Concept at New York International Auto Show (Mar. 28, 2018) (https://www.genesisnewsusa.com/en-us/releases/88).
27 Jonathan Kent, *Malaysia Car Thieves Steal Finger*, BBC News (Mar. 31, 2005), http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.
28 Innovative Ignition Systems, *Biometric Start Systems: Bio-800* (last visited Nov. 13, 2018), http://www.innovativeignitionsystems.com/bio-800.
29 US Patent Application Pub. No. 2016/0300410 A1 (filed Apr. 10, 2015).
30 NVIDIA, Self-Driving Cars - NVIDIA DRIVE IX, https://www.nvidia.com/en-us/self-driving-cars/drive-ix/ (last visited Nov. 19, 2018); see also NVIDIA DRIVE IX, YouTube, https://www.youtube.com/watch?v=v38TVn-Jsyw (demonstrating facial recognition to open car trunk and eye-tracking to warn of distracted or drowsy driving).
31 Eric A. Taub, *Sleepy Behind the Wheel? Some Cars Can Tell*, N.Y. Times (Mar. 16, 2017), https://www.nytimes.com/2017/03/16/automobiles/wheels/drowsy-driving-technology.html.
32 See Joseph Volpe, *Mitsubishi Electric's EMIRAI Concept Goes Back to the Future, Refuses to Fly (Video)*, Engadget (Dec. 10, 2011), https://www.engadget.com/2011/12/10/mitsubishi-electrics-emirai-concept-goes-back-to-the-future-re/ (see embedded video, *also available at* https://www.youtube.com/watch?v=ZX8I5wiFdLo); Kristen Hall-Geisler, *How Will the Car of the Future Use Biometrics?*, HowStuffWorks, https://auto.howstuffworks.com/future-car-biometrics.htm.
33 Press Release, Delta ID Inc., Delta ID Introduces Iris Scanning Technology for In-Car Biometrics and Secure Autonomous Driving at CES 2017 (Jan. 5, 2017), https://www.prnewswire.com/news-releases/delta-id-introduces-iris-scanning-technology-for-in-car-biometrics-and-secure-autonomous-driving-at-ces-2017-300386174.html.
34 See '410 Publication.
35 Voice Recognition Installed in More than Half of New Cars by 2019, IHS (Mar. 19, 2013), https://technology.ihs.com/427146/voice-recognition-installed-in-more-than-half-of-new-cars-by-2019.
36 Katie Burke, Alexa, Do I Need A Virtual Assistant in the Car?, Automotive News (Jan. 22, 2017), http://www.autonews.com/article/20170122/OEM06/301239846/alexa-do-i-need-a-virtual-assistant-in-the-car.
37 Murray Slovak, Gesture Recognition, Proximity Sensors Drive Advances in Automotive Infotainment, Avnet, https://www.avnet.com/wps/portal/us/resources/technical-articles/article/markets/automotive%20and%20transportation/gesture-recognition-proximity-sensors-drive-advances-auto-infotainment/ (last visited Nov. 15, 2018).

contact to a touchscreen. Sensors have been developed to recognize such in-car gestures, including those that register 3D movements and positional data of the hand and proximity sensing. Hyundai’s HCD-14 Genesis concept sedan demonstrated 3D gesture recognition for controlling the dashboard’s navigation and volume and changing radio stations.[38]

> *“Auto manufacturers are also integrating face and iris recognition technology with a vehicle camera system directed at the driver to detect fatigue or drowsiness.”*

38 Press Release, Hyundai’s HCD-14 Genesis Concept to be Showcased on Prestigious Concept Lawn and 2013 Pebble Beach Concours D’Elegance, Hyundai (Aug. 12, 2013), https://www.hyundainews.com/en-us/releases/1690.

III. United States

A. Biometric regulations

Although the adaptation of biometrics in technology has been increasingly incorporated into our daily lives (e.g. cellular phones, banking, computers, etc.), there has not been a commensurate proliferation of laws, on either the federal or state levels, that regulate how biometric data are collected or stored. Currently, there are only three states – Illinois, Texas and Washington – that have laws dealing specifically with protecting consumers' biometric information. Other states have chosen to include biometric data as a category of personal information protected under consumer privacy or data breach notification statutes. Nevertheless, unlike the specific laws covering biometric data or consumer privacy that require proactive steps to protect consumers' biometric information, the data breach notification statutes merely require disclosure of the data breach to affected parties.

(i) Illinois – Biometric Information Privacy Act

In 2008, Illinois became the first state in the US to pass legislation, the Biometric Information Privacy Act (BIPA),[39] regulating the collection and storage of biometric information. The statute limits the definition of "biometric identifier" to mean "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[40] BIPA also identifies, in a long list, materials that would not be considered biometric identifiers, including "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[41] The statute further defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[42] Thus, biometric information protected by BIPA would include any data or templates that result from the conversion of the captured biometric identifiers.

BIPA sets forth requirements for private entities relating to their retention, collection, disclosure, and destruction of an individual's biometric identifiers or biometric information. These private entities: (1) must have retention and destruction schedules in place and these written policies must be made available to the public; (2) must obtain the individual's written consent to collect the biometric data; (3) cannot profit off the biometric data – including by selling, leasing, or trading the data; (4) cannot disclose or disseminate the biometric data without the individual's consent or authorization; and (5) must "store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry" and "in a manner that is the same as or more protective than the manner

39 740 Ill. Comp. Stat. 14/1 et seq.
40 *Id.* at § 10.
41 *Id.*
42 *Id.*

Paul Keller
Partner, New York
Tel+ 1 212 318 3212
paul.keller@nortonrosefulbright.com

Jeff Richardson
Partner, Dallas
Tel+ 1 214 855 8121
jeff.richardson@nortonrosefulbright.com

Sue Ross
Sr. Counsel, New York
Tel+ 1 212 318 3280
sue.ross@nortonrosefulbright.com

Rachel Roosth
Senior Associate, Houston
Tel+ 1 713 651 3734
rachel.roosth@nortonrosefulbright.com

Jenny Shum
Senior Associate, New York
Tel+ 1 212 318 3362
jenny.shum@nortonrosefulbright.com

in which the private entity stores, transmits, and protects other confidential and sensitive information."[43] The private entities are not permitted to store the biometric identifiers or information past the time where the initial purpose of the collection is satisfied or for more than three years after the individual's last interaction with the private entity.[44]

One unique aspect of BIPA is that it grants a right of action to any individual harmed by a violation of the law, and each violation can incur penalties ranging from $1000 to $5000 (or actual damages), depending on whether the violation was a result of negligence or intentional or reckless action on the part of the private entity, plua attorneys' fees.[45] As a result of this provision, multiple class action suits have been filed alleging improper collection of facial geometry or fingerprints. The first wave of such suits were filed in 2015 against social media and technology companies, including Shutterfly, Facebook, and Google, alleging that their respective use of facial recognition technology was used without the plaintiffs' consent and was therefore in violation of BIPA.[46] Many more class action suits have been filed since, with some employee suits alleging that employers' collection of fingerprint data, used to track employees' time and authenticate employees' identity, violated BIPA.[47]

Due to the restrictive nature of BIPA, which requires written consent from the individual before collection of any biometric data, and the potential for large penalties as a result of class action suits, companies have taken care to avoid potential liability. For example, Google denied access to its Google Art & Culture mobile application (app) to Illinois residents (as well as Texas residents).[48] The app contains a feature, the Art Selfie, which asks the user to upload a picture of the user (the "selfie") and then compares the selfie to works of art and identifies works of art that most closely match the selfie.[49] Similarly, in Illinois, the smart home technology company Nest disables the facial recognition capability in its smart doorbell.[50]

43 740 Ill. Comp. Stat. 14/15.
44 *Id.*
45 *Id.* at § 20.
46 *Rivera v. Google, Inc.*, No. 16-CV-02714 (N.D. Ill. Dec. 29, 2018) (alleging lack of required disclosure and consent); *In re Facebook Biometric Info. Privacy Litig.*, No. 15-cv-3747 (N.D. Cal.) (alleging lack of required disclosure and consent); *Norberg v. Shutterfly Inc.*, No. 15-CV-5351, 2015 WL 9914203 (N.D. Ill. 2015) (alleging the collection of facial geometry of individuals without required notice or consent).
47 *See e.g. Sekura v. Krishna Schaumburg Tan, Inc.*, No. 1-18-0175 (Ill. App. Ct. Sept. 28, 2018) (lack of required disclosure); *Aguilar v. Rexnord, LLC*, No. 17-CV-9019 (N.D. Ill. July 3, 2018) (lack of required disclosure and consent); *Howe v. Speedway LLC*, No. 17-CV-07303, 2018 WL 2445541 (N.D. Ill. May 31, 2018) (lack of required disclosure and consent).
48 Alix Langone, *You Can't Use Google's New Selfie Art App in These States*, Time (Jan. 17, 2018), http://time.com/5106798/google-selfie-app-not-work-states.
49 https://play.google.com/store/apps/details?id=com.google.android.apps.cultural&hl=en_US
50 Ally Marotti, *Proposed Changes to Illinois' Biometric Law Concern Privacy Advocates*, Chicago Tribune (Apr.10, 2018), https://www.chicagotribune.com/business/ct-biz-illinois-biometrics-bills-20180409-story.html. Nest is owned by Alphabet, which is also the parent company of Google.

> *"One unique aspect of [the Illinois law] is that it grants a right of action to any individual harmed by a violation of the law, and each violation can incur penalties..."*

(ii) Texas – Capture or use of biometric identifier

Texas, in 2009, codified its law requiring notice of collection and consent by individuals before biometric identifiers can be captured and used for commercial purposes.[51] As with the Illinois BIPA, biometric identifiers were only defined as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[52] Unlike BIPA, which also extends protection to biometric information that results from the conversion of biometric identifiers, the Texas statute does not include a similar definition of or clause for biometric information. Under the Texas statute, notice and consent are required prior to the capture of any biometric identifiers. Moreover, companies or individuals cannot profit by selling or leasing the collected biometric data and cannot disclose the biometric identifiers to a third party. Mirroring BIPA requirements, the storage, transmission, and protection from disclosure of biometric identifiers requires that reasonable care to be taken and that it be done in the same manner that the company or person treats its own confidential information. Contrary to BIPA, no written consent is required for the collection of biometric data, and the destruction of biometric data must be destroyed "within a reasonable time, but no later than the first anniversary of the date the purpose for collecting the identifier expires."[53]

There is also no private right of action for individuals against private entities that violate the law. Only the Texas attorney general may bring action against anyone that violates this law and the civil penalty for each violation is capped at $25000.[54]

51 Tex. Bus. & Com. Code Ann. § 503.001.
52 *Id.* at § 503.001(a).
53 See *id.* at §§ 503.001(b), (c)(3).
54 *Id.* at § 503.001(d).

(iii) Washington – Biometric identifiers

Washington passed its biometric privacy statute in 2017.[55] It requires businesses to give notice to and acquire consent from an individual prior to "enrolling or changing the use of that individual's biometric identifiers in a database."[56] The definition of "biometric identifier" in Washington's statute is broader than those used in Illinois's and Texas's statutes. Washington's statute defines biometric identifiers to encompass "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[57] Note, however, biometric identifiers do not include "a physical or digital photograph, video or audio recording or data generated therefrom."[58]

As with the Texas statute, the Washington statute differs from Illinois's BIPA by not requiring written consent prior to the collection of the biometric data. Deviating from Illinois and Texas, the Washington statute states that biometric identifiers can be retained "no longer than is reasonably necessary" to provide the services that the biometric identifier was collected for or to protect against or prevent fraud or criminal activity.[59] It also does not permit a private right of action against businesses that violate the law and only authorizes the Washington attorney general to enforce the law.[60] Also unlike the other two states' biometric privacy laws, the Washington statute does not include any language with respect to monetary penalties for each violation of the law.

Interestingly, the Washington statute carves out a security exception to providing notice and obtaining consent. An entity is not required "to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose."[61] Such a "security purpose" would include preventing shoplifting, fraud, misappropriation or theft of a thing of value, and "other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person."[62]

55 Wash. Rev. Code Ann. § 19.375, et seq.
56 *Id*. at § 19.375.900.
57 *Id*. at § 19.375.010.
58 *Id*.
59 Wash. Rev. Code Ann. § 19.375.020(4)(b).
60 See *id*. at § 19.375.030.
61 *Id*. at § 19.375.020.
62 Id. at § 19.375.010.

(iv) California – California Consumer Privacy Act of 2018

California enacted a consumer privacy law on June 28, 2018 (amended September 23, 2018), the California Consumer Privacy Act (CCPA), that protects the personal information, broadly defined to encompass biometric information, of California residents that is collected or transmitted by businesses.[63] Unlike the statutes discussed above, the CCPA is not specifically directed towards safeguarding consumers' biometric information. However, the CCPA's definition of biometric information is more comprehensive and broader than those biometric statutes. Biometric information, as defined by CCPA, means:

> an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.[64]

The CCPA grants California residents many rights associated with controlling the collection and dissemination of their personal information. Consumers have the right to: (1) know what personal information is being collected; (2) know whether personal information is being sold or disclosed, what categories of personal information was sold or disclosed (including what "specific pieces of personal information" the business had collected), and to whom the information was sold or disclosed to; (3) prevent the sale of their personal information ("the right to opt-out"); and (4) request that a business delete any personal information collected.[65] The CCPA also forbids a business from discriminating against consumers who exercise their rights under the CCPA, including by charging different prices or rates or providing a different level or quality of goods and services.[66] Additional compliance requirements are also laid out in the CCPA, including disclosure rules and deadlines for delivery of requested personal information.

63 California Consumer Privacy Act, Cal. Civ Code § 1798.100 et seq.; amended SB 1121 on Sept. 23, 2018
64 CCPA § 1789.140(b)
65 CCPA § 1798.100 et seq.
66 CCPA § 1789.125

The regulations are applicable to any business that "does business in the State of California," collects consumers' personal information and meets at least one of the following thresholds: (A) has annual gross revenues in excess of twenty-five million dollars ($25,000,000); (B) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or (C) derives fifty percent or more of its annual revenues from selling consumers' personal information.[67] Businesses that are located outside of California but meet the above criteria would be subject to the CCPA.

The statute authorizes a private right of action if there is a data breach of unredacted or unencrypted personal information and the company failed to implement and maintain reasonable security measures.[68] The civil damages would be between $100 and $750 per consumer per incident or the actual damages incurred. Additionally, the California attorney general is also authorized to file suit with civil penalties of $2,500 for each violation or $7,500 for each intentional violation.[69] Businesses are provided with thirty days after receiving notice of noncompliance to cure any alleged violation.

(v) Data breach notification statutes

Unlike states that have enacted laws specifically addressing biometric data, other states have data breach notification statutes that also include biometric data as protected personal information.[70] For example, in 2017, Delaware addressed the issue of biometric data by amending its data breach disclosure law to expand the definition of protected personal information to include "unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes."[71] These data breach notification statutes merely require disclosure of the data breach to affected parties, with varying penalties for such breaches, and generally do not require any proactive steps to be taken to protect the information itself.

(vi) US industry security standards for biometrics

The FIDO ("Fast Identity Online") Alliance, a non-profit industry consortium that was formed to standardize security specifications for strong authentication (e.g. authentication requiring at least two forms of verification, which may include biometric information) across devices, launched a Biometrics Certification Program on September 6, 2018.[72] The FIDO Alliance membership consists of hundreds of global technology companies, including Google, Intel, and Microsoft.[73] The membership does not currently include any of the major automotive manufacturers. The Biometrics Certification Program is intended to "certify that biometric subcomponents meet globally recognized performance standards [i] for biometric recognition performance and Presentation Attack Detection (PAD) [ii] and are fit for commercial use."[74] This standardization of biometric technology security specifications, if universally adopted, should assure consumers and manufacturers that the biometric components in their products are secure and can repel attempts to bypass the biometric systems.

(vii) Biometrics regulations and autonomous vehicles

Due to the current lack of uniform regulations regarding biometrics and the varying data breach notification statutes amongst the states, and the likelihood of additional legislation in the future, automobile manufacturers should take care to consider each individual state's collection, destruction, disclosure, and privacy requirements when incorporating biometric technology into their AVs.

67 CCPA § 1789.140(c)
68 CCPA § 1789.150
69 CCPA § 1789.155
70 Arizona - Ariz. Rev. Stat. § 44-7501 (2006), as amended (2007, 2016, 2018); Colorado - Colo. Rev. Stat. Ann. § 6-1-716 (2006), as amended (2018); Iowa - Ia.Code Ann. §§ 715C.1 et. seq. (2008), as amended (2014); Louisiana - La. Rev. Stat. § 51:3071-3077 (2005), L.A.C. 16:III.701; Maryland - Md. Code Ann., Com. Law § 14-3501-3508 (2007); as amended (2017); Nebraska - Neb. Rev. Stat. §§ 87-802 to -806 (2006), as amended (2016); New Mexico - 2017 H.B. 15, Chap. 36; North Carolina - N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009); South Dakota - Senate Bill 62 (2018); Wisconsin - Wis. Stat. Ann. § 134.98 (2006); as amended (2008); and Wyoming - Wyo. Stat. Ann. §§ 40-12-501, 40-12-502 (2015).
71 An Act To Amend Title 6 Of The Delaware Code Relating To Breaches Of Security Involving Personal Information, 6 Del. C. §§12B-101(4)(a)(11), amended Aug. 17, 2017.
72 Press Release, FIDO Alliance, FIDO Alliance Launches Biometrics Certification Program (Sept. 6, 2018) (https://fidoalliance.org/fido-alliance-launches-biometrics-certification-program/). The FIDO Alliance membership consists of hundreds of global technology companies (https://fidoalliance.org/overview/).
73 FIDO Alliance, FIDO Members (https://fidoalliance.org/members/). (last visited Fed. 15, 2019)
74 *Id.*

B. Patent landscape - Biometrics in autonomous vehicles

Patents relating to biometric modalities in the US number well over 60000, with over 52000 additional patent applications filed. As might be expected, the greatest number of biometric patents and patent applications relate to the more well-established biometric modalities, e.g. fingerprints, facial recognition, and retinal scanning. As more of these biometric modalities are incorporated into next generation AVs, the number of related patent filings has also increased correspondingly.

(i) Leaders in biometric patents in the automotive

The patent landscape in the US for biometrics with applicability in the automotive industry is robust and growing rapidly. Over the last 30 years, there have been over 16000 patents issued that relate to biometrics and automobiles or AVs. Much of this growth has come in the past decade, with a eight-fold increase in these biometric patents issued. And in the last 20 years, over 15000 patent applications have been filed for inventions relating to the same. Interestingly, many of the top applicants for patents in biometrics in the automotive space have not been the major automotive companies. Instead, many of these top applicants are more traditionally known as technology companies.

As can be seen in the table below of the top 20 assignees with such patents and patent applications, IBM, Google, Microsoft, Apple, and Samsung are in the top five of both of these lists in terms of absolute numbers of patents granted and patent applications filed. Samsung has invested significantly in both biometrics and self-driving technologies.[75] IBM is also involved in developing AVs and has a research group dedicated to biometrics.[76] Microsoft, in contrast, is not directly involved in developing AVs, but is instead focusing on providing its software and technology to auto manufacturers that are developing such vehicles.[77] Google, which has heavily invested in the development of autonomous vehicles under its subsidiary Waymo, has 410 patents issued and another 502 patent applications pending. (See Table 1.) Apple also has an AV program and has 346 issued patents and 639 patent applications pending at the Patent and Trademark Office (USPTO). For example, a recently published patent application, filed originally on Feb. 3, 2017, revealed that Apple was interested in incorporating mobile biometric technology, e.g. facial or fingerprint recognition technology (like its proprietary Face ID and Touch ID), to unlock a vehicle.[78] Of the more traditional car companies, Ford Motor Company (Ford) appears on both lists and has expressed interest in putting biometric sensors in their cars.[79] General Motors Company (GM) also has a significant number of patent applications relating to biometrics pending.

Non-practicing entities also appear to be well-positioned with large numbers of US patents and patent applications in the biometrics and automotive space. For example, American Vehicular Sciences, LLC is a subsidiary of Acacia Research Corporation, a company that focuses on patent licensing by partnering with patent owners, and holds 125 patents involving biometrics and the automobile industry. Similarly, Liberty Peak Ventures LLC has a large portfolio of 186 patents and 141 patent applications pending.

75 Press Release, Samsung, Samsung Electronics Expands Commitment to Autonomous Driving Technology (Sept. 14, 2017), https://www.samsung.com/us/ssic/press/samsung-electronics-300-m-automotive-innovation-fund/; Vineeth Joel Patel, *Having Multiple Partnerships Will Help Samsung Become an Autonomous Tech Leader*, FutureCar (May 15, 2018), http://www.futurecar.com/2263/Having-Multiple-Partnerships-Will-Help-Samsung-Become-an-Autonomous-Tech-Leader.

76 Susane Keohane, *How Inventing Became a Passion: Developing Autonomous Vehicles to Help Support Healthy Aging and People with Disabilities* (Mar. 15, 2018), IBM, https://www.ibm.com/blogs/research/2018/03/developing-accessible-autonomous-vehicles/; see Biometrics, IBM Research, https://researcher.watson.ibm.com/researcher/view_group.php?id=1913 (last visited Nov. 13, 2018).

77 Andrew Meola, *Microsoft is Approaching Self-Driving Cars in a Unique Way*, Business Insider (June 6, 2016 2:23 PM), https://www.businessinsider.com/microsoft-is-approaching-self-driving-cars-in-a-unique-way-2016-6.

78 US Patent Application No. 16/075,442 (Publication No. 20190039570; filed Feb. 3, 2017, published Feb. 7, 2019)

79 *See* Table ___ (Top 20 Assignees with... biometrics in automobiles); Jen Wieczner, *Why Ford Wants to Put Biometric Sensors in Your Car*, Fortune (May 4, 2017), http://fortune.com/2017/05/03/ford-self-driving-car-biometric/.

	US Patents		US Patent Applications	
	Assignees	**Number**	**Assignees**	**Number**
1	Samsung	549	Samsung	1605
2	International Business Machines	426	International Business Machines	760
3	Google	410	Apple	639
4	Microsoft	354	Microsoft	612
5	Apple	346	Google	502
6	AT&T	297	Intel	455
7	IGT	292	IGT	453
8	Diebold	287	AT&T	388
9	Liberty Peak Ventures LLC	186	LG	351
10	Intel	184	Qualcomm	302
11	Qualcomm	174	Liberty Peak Ventures LLC	301
12	Digimarc	172	Sony	247
13	Fitbit	163	Ford Motor Company	239
14	Bally Technologies	139	Bank of America	207
15	Amazon	138	Elwha	205
16	LG	138	Fitbit	198
17	Ford Motor Company	137	Digimarc	187
18	American Vehicular Sciences LLC	125	General Motors Company	186
19	Verizon	125	Bally Technologies	179
20	Sony	117	Visa	177

Table 1: Top 20 Assignees with Most US Patents or US Patent Applications Relating to Biometrics in Automobiles.

(ii) Leaders in patents on biometrics in AV

Many of the major auto manufacturers are currently in various stages of research and development on AVs, either independently or in partnership with technology companies.[80] Nevertheless, the companies that are developing or incorporating biometrics into AVs and seeking to protect their intellectual property generally are not the automotive manufacturer, with the exception of Ford and GM. This is reflected in Table 2, which shows that most of the patents and patent applications relating primarily to biometrics in AVs belong to technology or independent automotive research and development companies that are deeply invested in developing AVs and related technologies, including the incorporation of biometrics. For example, Veniam, Inc. is a startup technology company that aims to provide "[t]he networking solution for AVs and future mobility."[81] Veniam has the largest number of issued patents and filed patent applications for inventions relating to biometrics in AVs. Similarly, Z Advanced Computing, Inc. is a software startup company that focuses on the use of artificial intelligence with biometrics and AVs.[82] Intelligent Technologies International, Inc. and Automotive Technologies International, Inc. are related companies that focus on automotive safety research and development.[83] In contrast to the broader category of patents and patent applications relating to biometrics in the automobile industry (Table 2), here – where the inventions claimed relate to biometrics in AVs – non-practicing entities have not yet established a presence in the field.

	Owners	Patents	Applications	Total
1	Google/Waymo	247	313	560
2	Samsung	105	429	534
3	AT&T	181	234	415
4	LG	87	246	333
5	Microsoft	110	197	307
6	Diebold	184	115	299
7	Intel	69	229	298
8	Digimarc	135	141	276
9	American Vehicular Sciences LLC	123	152	275
10	International Business Machines	87	153	240
11	Apple	74	151	225
12	Ford Motor Company	78	143	221
13	Autoconnect Holdings LLC	55	145	200
14	GM	54	128	182
15	Veniam, Inc.	54	124	178

Table 2: Top 15 Assignees with Most US Patents or US Patent Applications Relating to Biometrics in Autonomous Vehicles.

80 Audi A8; Volvo XC90 (Zenuity); BMW i8 at CES 2016 and (BMW iNEXT); Ford (Argo); GM (Chevy Bolt); Honda and Waymo; Hyundai & Aurora and see CES 2019; Tesla.
81 Products. https://veniam.com/autonomous-vehicles (last visited Feb. 15, 2019).
82 http://www.zadvancedcomputing.com/ [fix cite]
83 https://iti-i.com/about-us and https://ati-i.com/about-us-3/; both owned by David S. Breed [fix cite]

The number of patents issued and patent applications filed on inventions involving biometrics in AVs has slowly increased over the past decade. In 2017, however, the numbers of patents and patent applications dramatically increased, with the number of patents granted and patent applications filed increasing by about 50% from the previous year. See Table 3.

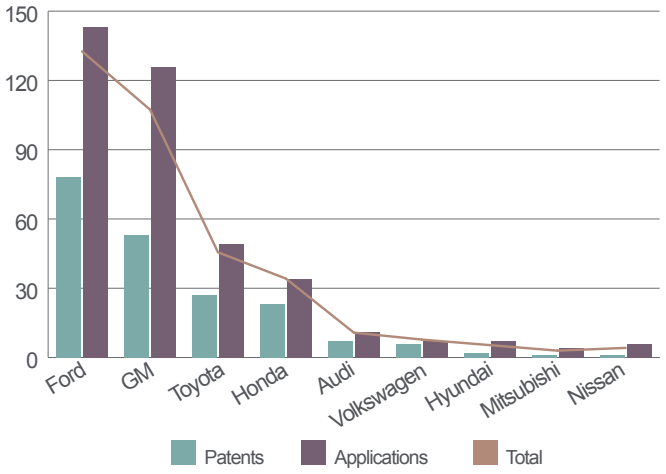
Year	Granted patents	Applications published
2009	146	133
2010	243	131
2011	282	194
2012	293	160
2013	415	255
2014	432	364
2015	506	556
2016	596	956
2017	867	1493
2018	1115	1245

Table 3. Biometrics in autonomous vehicles: Total number of patents granted and applications published in 2008-2018.

This upward trend will likely continue as there have been 675 patents granted and over 1190 such patent applications published in just the first six months of 2019 (on track for over 1300 patents granted and nearly 2400 published patent applications for the year).

Of the traditional auto manufacturers, Ford, GM, Toyota, and Honda currently have the largest number of patents and patent applications relating to biometrics in AVs. Figure 1. As more auto manufacturers begin to incorporate biometrics into their proprietary technologies, it is likely that they will seek to protect their substantial investments in the AV space by increasing their own patent filings.[84] For example, in 2018, Ford created Ford Autonomous Vehicles LLC to "accelerate[ ] the integration and application of technology across its industrial system."[85]

Figure 1. Biometrics in autonomous vehicles: Patents and patent applications assigned to auto manufacturers.



(iii) Future risks of patent litigation and trade secret misappropriation

Although there have been litigations on patent infringement and trade secret misappropriation relating to AV technologies, and patent infringement litigations relating to biometric technologies in other product spaces (e.g. cellular phones), there have not yet been similar claims made with respect to biometric technologies in AVs. Nevertheless, in view of the ever-increasing numbers of patent applications filed and patents granted for biometric technologies in the AVs space, it is likely that the risk of patent litigations will also correspondingly escalate. There is also a risk that non-practicing entities will utilize their existing automotive biometric technology patent portfolios and seek to assert them against companies working on AVs that include biometric technologies.

As the AV industry matures, the automotive industry may adopt the same solutions for potentially overlapping intellectual property that the technology and software industries developed to end high-stakes disputes, the identification of standard-essential patents (SEPs) and the licensing of SEPs on Fair, Reasonable, and Non-Discriminatory

84 See Bret Kenwell, *GM, Ford Bump Up Investments in Electric and Autonomous* (Mar. 24, 2019), TheStreet, https://www.thestreet.com/lifestyle/cars/gm-ford-invest-in-electric-and-autonomous-14904586.

85 Press Release, Ford Motor Company, Ford Creates 'Ford Autonomous Vehicles LLC'; Strenthens Global Organization to Accelerate Progress, Improve Fitness (July 24, 2018) (https://media.ford.com/content/fordmedia/fna/us/en/news/2018/07/24/ford-creates-ford-autonomous-vehicles-llc.html).

(FRAND) terms. In addition the automotive industry may create patent pools and enter into cross-licensing agreements to avoid damaging, expensive, and time-consuming litigations.

The risk of trade secret misappropriation is always a concern in technology fields, and this holds true for the AV industry. Although the concepts between capturing biometric information are well known, the proprietary algorithms are usually not publicly available. There has been significant crossover of personnel between the many companies working on AVs and that increases the risk of loss of trade secrets.[86] To preserve a potential trade secret misappropriation claim, AV manufacturers must ensure that the trade secret is not freely disseminated and that reasonable efforts are made to keep it secret.

Trade secret misappropriation claims can be filed under federal or state law. In Waymo LLC v. Uber Technologies, Inc., Waymo LLC ("Waymo"; the AV unit of Google's parent company Alphabet) filed suit alleging patent infringement of its laser-based scanning and mapping technology ("LIDAR"), trade secret misappropriation of subsequent and unpatented confidential LIDAR designs and technical information, and unfair competition against Uber Technologies, Inc. ("Uber"), OttoMotto LLC, and Otto Trucking LLC (together, "Otto").[87] Waymo claimed defendants violated both the federal Defend Trade Secrets Act ("DTSA") and California Uniform Trade Secrets Act ("California UTSA").[88] Waymo alleged that its former manager Anthony Levandowski had searched for and downloaded more than 14,000 proprietary files before his resignation from Waymo in 2016 and his formation of Otto, which was acquired by Uber six months later for $680 million. Waymo claimed that Uber was aware of Levandowski's possession of Waymo's files and was using Waymo's trade secrets and patented technology to develop its own LIDAR system. After five days of trial, the parties settled with Uber, granting Waymo 0.34 percent of Uber's stock, valued at about $245 million, and agreed that Uber would not use Waymo's confidential information in its self-driving technology.[89]

Trade secret misappropriation claims are not limited to only civil lawsuits but also can have criminal implications for theft of trade secrets, with the potential for up to ten years imprisonment.[90] In separate criminal suits filed six months apart by the Federal Bureau of Investigation ("FBI"), two engineers were charged with attempting to steal trade secrets relating to Apple Inc.'s AV project, Project Titan. In the first case, with charges filed on July 9, 2018, Xiaolang Zhang was a former Apple engineer who had worked on Project Titan and was arrested by the FBI as he was about to board a plane to China. Apple's database security team had identified suspicious network and download activity by Zhang in the days prior to a meeting where Zhang had informed Apple that he intended to return to China to be closer to his mother and that he would be working for Xiaopeng Motors, a Chinese electric car start-up company that was also working on AVs. Zhang was accused of downloading proprietary information containing trade secrets relating to Apple's AV project.[91] During interviews with Apple and the FBI prior to Zhang's arrest, he admitted to taking hardware (a Linux server and two circuit boards) and transferring confidential Apple files onto his wife's laptop. Zhang has entered a plea of not guilty, and the case is ongoing.

In the second criminal case, filed on January 22, 2019, Jizhong Chen is also accused of theft of trade secrets from Apple's AV project.[92] According to the complaint, Chen was seen taking photographs of the Apple work space by another Apple employee, who then reported Chen to Apple. When questioned by Apple's investigation team, Chen admitted to taking the photos and also making a back-up of his Apple work computer to his personal device, in violation of Apple policy. Chen granted Apple's investigators access to his personal devices and thousands of files containing Apple confidential information were found. Additional photographs of the interior of Apple's building were also found on his cell phone. Chen was immediately suspended, and Chen's employee and network access was terminated. Apple subsequently learned that Chen had applied for a job with a China-based AV company, which was also a direct competitor to Project Titan. Chen was arrested a day before he planned to leave for China. Chen has pled not guilty.

86 Examples of individuals from Waymo to Uber, Waymo to Apple, etc.
87 No. 3:17-cv-00939 (N.D. Cal. Feb. 23, 2017).
88 Defend Trade Secrets Act, 8 USC. § 1836, *et seq*.; California Uniform Trade Secrets Act, Cal. Civ. Code § 3426, *et seq*.
89 Cara Bayles, *Uber, Waymo Settle Trade Secret Case Amid Trial*, Law360, Feb. 9, 2018, https://www.law360.com/articles/1010900/uber-waymo-settle-trade-secret-case-amid-trial.
90 18 USC. § 1832.
91 US v. Zhang, D.I. 1, No. 5:18-cr-00312, N.D. Cal. July 9, 2018.
92 US v. Chen, D.I. 1, No. 5:19-cr-00056, N.D. Cal. Jan. 22, 2019.

In addition to theft of trade secrets, companies should also be wary of economic espionage. While economic espionage cases have yet to be filed relating to AV technology, there are examples of such cases in other high-tech industries. For example, on September 27, 2018, the US government filed an indictment against Taiwan-based United Microelectronics Corp. ("UMC"), China state-owned Fujian Jinhua Integrated Circuit, Co., Ltd. ("Jinhua"), and three former employees of the US semiconductor company Micron Technology Inc. ("Micron") alleging economic espionage, theft of trade secrets, and conspiracies to commit economic espionage and theft of trade secrets.[93] The indictment alleges that former employees of Micron stole trade secrets relating to the design and manufacture of a memory storage device, dynamic random-access memory ("DRAM"), from Micron and then provided the information to UMC and Jinhua under the direction of Stephen Chen, the former president of Micron's Taiwan subsidiary, and others. After Chen left Micron, he became a Senior Vice President of UMC and then later became President of Jinhua in charge of its DRAM production facility. UMC and Jinhua had a technology cooperation agreement to develop DRAM technology, which Chen helped negotiate while at UMC. The US government valued the eight trade secrets alleged to have been stolen as worth at least $400 million and up to $8.75 billion. The US government also later filed for an injunction against the two companies to prevent the export of any products related to the alleged theft of trade secrets into the US and to prevent any further transfer of the trade secrets.[94] Micron itself had earlier filed a civil complaint against UMC and Jinhua alleging violations of DTSA and California UTSA.[95]

Although economic espionage charges were not asserted, on January 16, 2019, the US government filed a ten-count criminal indictment charging Huawei Device Co., Ltd. and Huawei Device USA, Inc. (collectively, "Huawei") for theft of trade secrets conspiracy, attempted theft of trade secrets, wire fraud, and obstruction of justice.[96] The indictment alleges that, beginning in June 2012, Huawei conspired to and attempted to steal T-Mobile USA, Inc. ("T-Mobile") trade secrets relating to its proprietary robotic phone testing system, called "Tappy."

The Tappy automated testing system simulates how people use the phone, with a robotic arm that touches the device screen, and tracks the phone's responsiveness and performance, among other things. The indictment states that Huawei was interested in developing its own robotic testing system in order to improve the quality of its phones and to pass Tappy's testing, and T-Mobile rejected overtures from Huawei to license or purchase the Tappy system.

Huawei USA engineers then proceeded to photograph the Tappy system and the software interface and provide access to the Tappy laboratory to an unauthorized Huawei China engineer, in violation of nondisclosure agreements. On May 29, 2013, a Huawei engineer also secretly removed one of the Tappy robotic arms from the laboratory. Upon questioning by T-Mobile, the Huawei engineer first denied taking the robotic arm and then claimed that it was a mistake and returned the robotic arm the next day, but only after taking photographs and detailed measurements of the robotic arm. T-Mobile then banned all Huawei personnel from the laboratory.

The indictment further alleges that, in order to preserve its relationship with T-Mobile, Huawei showed T-Mobile a redacted "Investigation Report" on Huawei's purported internal investigation that contained false statements that served to distance Huawei China from the theft of trade secrets and blamed the two engineers for what they termed "isolated incidents," when, in fact, the engineers' actions were instead directed and coordinated by Huawei USA and Huawei China. The indictment also disclosed that Huawei China had a bonus program that rewarded its employees for stealing competitors' confidential information. Huawei has denied the allegations in the indictment. Previously, T-Mobile won a $4.8 million civil suit against Huawei for breach of contract and misappropriation of trade secrets relating to the Tappy system.[97]

93 US v. United Microelectronics Corp., D.I. 1, No. 3:18-cr-00465, N.D. Cal. Sept. 27, 2018.
94 *US v. United Microelectronics Corp.*, D.I. 1, No. 5:18-cv-06643, N.D. Cal. Nov. 1, 2018.
95 Micron Tech., Inc. v. United Microelectronics Corp., D.I. 1, No. 3:17-cv-06932, N.D. Cal. Dec. 5, 2017.
96 *US v. Huawei Device Co., Ltd.*, D.I. 1, No. 2:19-cr-00010, W.D. Wash. Jan. 16, 2019.
97 *T-Mobile USA, Inc. v. Huawei Device USA, Inc.*, D.I. 1, No. 2:14-cv01351, W.D. Wash. Sept. 2, 2014.

C. Biometrics and automobile insurance

In our previous analyses of the effects of AVs on the insurance industry, we emphasized that insurers can be—and have been—leaders in adapting to the development of AV technologies. Insurers' roles regarding biometric technologies in AV is no different. Automobile insurance companies are developing ways to take advantage of biometric technologies in vehicles, including by using biometric technologies to monitor drivers and investigate claims.

(i) Monitoring drivers

Automobile insurers have been using technology to monitor driving behaviors for over 20 years, but biometric technologies can expand that practice. Currently, several insurance companies offer programs through which drivers agree to install monitors in their cars in exchange for potentially lower insurance rates. The monitors track data that insurance companies can use to determine how safely the car has been operated. These technologies monitor the drivers indirectly, by extrapolating the drivers' behaviors from the performance of their vehicles.

In contrast, biometric technologies give insurers the opportunity to monitor the drivers themselves. Biometric data can help insurers determine who is operating a vehicle and what physical or emotional state that person is in. For instance, State Farm has obtained patents for systems to assess a driver's impairment, such as anxiety, intoxication, illness, or injury.[98] According to these patents, sensors could monitor the driver's gaze, movement, heart rate, blood pressure, grip pressure, body temperature, and vocal pattern, among other things, to determine whether the driver is in an impaired state. Another State Farm patent describes a system to adjust insurance rates based on any detected impairment of the driver.[99] As these patents suggest, biometric data may allow insurers to adjust their insurance rates based on the actual behavior of vehicle operators.

But the utility of monitoring drivers through biometric data extends beyond insurance pricing. Insurers may also increase safety by responding to biometric data. A Hartford Insurance patent describes a system that uses biometric information to load a profile for the vehicle operator, and then impose restrictions on the vehicle's operation based on that profile.[100] The system could require the driver to pass a breathalyzer before operating the car, prevent the car from exceeding a maximum speed, or cause the car to become inoperable outside of a particular geographic area. As another example, State Farm's systems for detecting a driver's impaired state would also respond to impaired states.[101] Depending on the kind and degree of impairment, the systems could select an appropriate response, such as playing music, releasing a scent, providing visual or auditory alerts, altering the vehicle's internal lighting, blasting hot or cold air at the driver, or limiting the inflow of external stimuli like text messages and phone calls. The systems might encourage the driver to stop the vehicle by suggesting nearby destinations to visit, and the system could even provide coupons for those destinations. By responding to the operator's impairment, the insurer may be able to promote safer operation of the vehicle.

(ii) Investigating claims

When claims are made on a policy, biometric data may help insurers investigate and gather relevant evidence. Insurers may be able to obtain biometric data directly from the car that would reveal who was driving, how many people were in the car, whether the driver was alert, distracted or impaired, and how attentive the driver appeared. The biometric data could include vital medical information of vehicle occupants, like heart rate, blood pressure, and body temperature. By collecting this data directly from the car, the insurer may be able to obtain the information quickly and check it against information provided by other sources.

Biometric data may also help insurance companies determine if a claim falls under a policy exclusion. For example, many auto insurance policies contain a public or livery conveyance exclusion that excludes coverage for vehicles used to transport people for money. Biometric data could reveal the number or frequency of new individuals entering a vehicle, and insurers could assess whether that information appears consistent with the vehicle's use as a taxi, limousine, Uber, or Lyft. This information could suggest whether the public or livery conveyance exclusion is applicable. As another example, some states permit named driver exclusions, which allow policyholders to exclude certain individuals from their insurance (like a household member with a bad driving record) in order to obtain a better rate. Biometric data may tell insurers whether the driver involved in an accident was indeed the policyholder, or instead an excluded household member. In these ways, insurers can use biometric data to make more accurate coverage decisions.

98 US Patent Nos. 9,908,530 (Mar. 6, 2018) and 10,121,345 (Nov. 6, 2018).
99 US Patent No. 10,163,163 (Dec. 25, 2018).
100 US Patent No. 9,070,168 (Jun. 30, 2015).
101 US Patent Nos. 9,908,530 (Mar. 6, 2018) and 10,121,345 (Nov. 6, 2018).

D. Conclusion

Biometric technologies are increasingly being integrated into the mundane aspects of daily life, from completing financial transactions via ATM or online access to unlocking laptops and cellphones. There are a multitude of biometric physical and behavioral modalities that have been used for identification and authentication. While physiological traits such as fingerprint and facial recognition are well-recognized and their potential uses covered by an ever increasing number of patents, biometric systems based on gait and gesture recognition continue to be developed and patented. The automobile industry is embracing this trend and working on moving biometric controls in automobiles, such as gesture recognition, from the concept stage to mass production. However, given the increasing number of patents and patent applications on inventions relating to biometrics, and biometrics in the automotive arena, manufacturers should carefully consider whether there is existing intellectual property that covers the manufacturer’s intended uses and proceed accordingly. Care should also be taken by AV manufacturers to protect and secure confidential and proprietary information from competitors and their own employees.

Patents relating to biometric modalities in the US number well over 60000, and with over 52000 additional patent applications filed.”

IV. Australia

Automated vehicle technology is likely to produce and retain data about vehicle behavior and vehicle occupants. Some of that data will sit only in-vehicle. However, some will be shared with and supplemented by information shared through Co-operative Intelligent Transport Systems (C-ITS) that allow vehicles to communicate directly with other vehicles and infrastructure, such as traffic signals. The prospect of this data creation, storage and sharing becomes increasingly significant when it is appreciated that AVs are one of many consumer devices likely to utilise biometric measurement and analysis.

Building on the fundamental analysis set out in chapter II to this report, this chapter will explore some of the biometric issues that are particular to the Australian AV context.

First, we will examine the steps that federal and state governments are taking to ensure they safeguard personal data obtained from an automated vehicle directly or otherwise through management of a C-ITS. Second, we will briefly examine intellectual property issues arising from biometric information. Finally, we will consider how biometric based technology has the capacity to improve safety and the role it may play in the liability regime likely to apply to AVs.

The reader should take two ideas from this chapter:

1. The Australian government is well-positioned in respect of laws to protect the privacy of personalized biometric data collected through the AV networks by the time the networks go live. Attention should be focussed on the rules for information sharing between federal and state governments, and between government agencies of either state or federal government.

2. Biometric analysis in AVs will tend to make harmful driving less prevalent, in particular in the heavy vehicle context.

Michael Sullivan
Partner, Sydney
Tel+ 61 2 9330 8886
michael.sullivan@nortonrosefulbright.com

Jackie O’Brien
Partner, Sydney
Tel+ 61 2 9330 8515
jackie.obrien@nortonrosefulbright.com

Lauren Holz
Associate, Sydney
Tel+ 61 2 9330 8226
lauren.holz@nortonrosefulbright.com

Ernest van Buuren
Partner, Brisbane
Tel+ 61 7 3414 2276
ernest.van.buuren@nortonrosefulbright.com

Peter Mulligan
Partner, Sydney
Tel+ 61 2 9330 8562
peter.mulligan@nortonrosefulbright.com

Harry Lawless
Associate, Sydney
Tel+ 61 2 9330 8875
harry.lawless@nortonrosefulbright.com

A. Regulatory update

In August 2019, Australia's Transport and Infrastructure Council will consider recommendations from the National Transport Commission to address privacy challenges arising from C-ITS and AV technology. The National Transport Commission's preferred option is to agree on broad principles on limiting government collection, use and disclosure of C-ITS information.

Also in August 2019, consultation will close on the consultation Regulation Impact Statement released by the National Transport Commission in July 2019. That document examines the roles of different parties in the safety of automated vehicles after market entry (in-service) and any additional duties which should apply to them. It also examines the institutional and regulatory arrangements to support any additional duties. Relevant to this chapter, it can be expected that duties in relation to data security will be imposed on in-service parties.

This recent work builds on a broader reform program undertaken by the National Transport Commission and other stakeholders which aims to develop end-to-end regulation to support the safe, commercial deployment and operation of fully automated vehicles. Other streams completed or ongoing relate to review of insurance schemes; development of enforcement guidelines; and safety criteria for first supply of AVs.

B. Government collection of data

Data will be the linchpin regulatory issue arising from the expected spread of biometrics in AVs. In participating in C-ITS, government and its agencies will become the custodians of new kinds of data, and will need to develop systems for its responsible use and custody. The capture of biometric data will present unique privacy and security challenges. Government also may see utility in getting access to AV data that is not ordinarily shared through a C-ITS framework.

The current law in Australia imposes privacy safeguards by stipulating processes for how state and federal governments must deal with information that meets the definition of "personal information" and, in some jurisdictions, "sensitive information." At the federal level, for example, the *Privacy Act 1988 (Cth)* governs the treatment of "personal information" by private and Commonwealth public sector entities. Various pieces of legislation also apply at a state and territory level, primarily regulating the use of "personal information" and/or "sensitive information" by state and territory agencies. Where the distinction between "personal information" and "sensitive information" exists, the latter is generally treated as a special subset of "personal information" to which more stringent protections apply. The National Transport Commission, in its discussion paper on regulating government access to C-ITS and AV data, has identified that most of the information generated in the C-ITS will be "personal information."[102] Some of this information, like the biometric information used to gain access to the vehicle (equivalent to fingerprint access to a mobile phone) would also be classified as "sensitive information" (at least in the Commonwealth jurisdiction), being "biometric information that is to be used for the purpose of automated biometric verification or biometric identification."[103]

> *"...biometric information used to gain access to the vehicle (equivalent to fingerprint access to a mobile phone) would also be classified as "sensitive information" (at least in the Commonwealth jurisdiction)..."*

In previous editions of this white paper we have canvassed the privacy law issues associated with data meeting the definitions of "personal information" or, in some jurisdictions, "sensitive information." At the federal level, for example, "sensitive information" can generally only be collected with the express consent of the relevant individual unless certain exceptions apply, key among these being where Australian law requires or authorizes such collection.[104]

102 *National Transport Commission*, 'Regulating government access to C-ITS and automated vehicle data' Discussion Paper (September 2018): <https://www.ntc.gov.au/Media/Reports/(614D48BA-F48B-38C8-FA90-A103E49A38CF).pdf> p 34 (hereafter, **NTC report**).
103 *Privacy Act 1988* s 6,
104 *Privacy Act 1988*, Schedule 1, Australian Privacy Principles 3.3, 3.4(a).

It is therefore relevant to consider the types of biometric data the National Transport Commission has identified will be collected in the C-ITS as a potential indicator of future directions in law reform. We extract the Commission's views on what we consider to be the most important: biometric characteristics of the actual driver:

- "Automated vehicles are likely to rely upon inward-facing cameras to monitor human driver alertness and behavior."[105]

- "Whole-of-cabin vehicle recordings could detect whether it is safe for the ADS to hand back control to a human (if manual vehicle controls exist)."[106]

- "Biological or health sensors can be used to monitor facial temperature, heart rate, breathing rate and glucose and biometric sensors could be used to recognize drivers and occupants to customize the driving experience... Automated vehicles may rely on these sensors to monitor driver alertness and behavior, including whether a human driver is losing attention or getting stressed. This could assist with determining whether the human driver is ready to take back control of the vehicle. However, they could also collect sensitive health and wellness information about users of automated vehicles (for example, emerging health issues such as a heart attack), including the driver and other occupants."[107]

Taken collectively, it is plausible that the entire interior of an AV and sounds from within it will be recorded, with the government having access to this data. The National Transport Commission has said that information generated by C-ITS could be collected and used by government to assist in:

- law enforcement;
- traffic management and road safety; and
- infrastructure and network programming.[108]

These are the societal goods that will need to be weighed against the intrusion on individual privacy. For example, in its submission in response to the National Transport Commission report, the Australian privacy regulator (the Office of the Australian Information Commissioner) has emphasized the importance of individual consent to the collection of "sensitive information," and noted that, in circumstances where it is not appropriate to obtain consent, increased "oversight, accountability and transparency" should be required.[109] Whatever the merits of this debate, what is clear is that the move towards AVs will actually decrease vehicle autonomy. In the 20th century, the car was a symbol of individuality. Nevertheless, a truly integrated system of AVs would actually operate a lot more like a series of private train carriages, by virtue of the interconnectedness that will be needed to enable them to share the roads safely. It is perhaps appropriate that an individual's expectations of privacy within them should shift accordingly.

C. Intellectual property

(i) Patents

The biometric technology likely to be integrated into the operation of an AV is a small part of a complex set of inter-related and inter-dependent technologies. Applicants have been filing and obtaining patents relating to biometric-dependent technologies for decades in Australia. The biometric aspect of AVs is therefore unlikely to require changes to Australian intellectual property. In the past several years, biometric technology has proved patentable in the context of other Australian industries.[110] There is little to suggest that biometrics in the particular context of AVs will be different.

(ii) Ownership of information and data collected by automated vehicles.

As canvassed in our last white paper, a big question which arises from the use of AV is "who owns all this data that will be generated?"

As noted above, Australian law does not recognise data, or mere information, itself as a type of property that can be owned, or bought and sold, but rather it is the confidentiality of that data that may be protected. Each case is to be assessed on its own circumstances, but if the person collecting the data guards its security and prevents it from reaching the public domain, it may have the necessary quality of confidence to qualify as confidential information. This is likely to be the vehicle manufacturer, for example, if the data is collected by on-board computers and securely transmitted back to the manufacturer for aggregating and analysis. This will depend on the steps

105 NTC report p 25.
106 NTC report p 26.
107 NTC report p 27.
108 NTC report p 38.

109 Office of the Australian Information Commissioner, Submission to the 'Regulating government access to C-ITS and automated vehicle data' Discussion Paper, 6 December 2018, <https://www.ntc.gov.au/Media/Reports/(E03DBF47-9B07-2B77-E6A3-64C797663917).pdf> p. 6.
110 http://pericles.ipaustralia.gov.au/ols/auspat/jumpToPage.do?searchID=588523A6-E7BD-446B-A384-5E201DEDBCF2&pageNavigation=first&resultsPerPage=10&firstRecordNo=451&lastRecordNo=460&resultsCount=461&currentPageNo=46&callingAction=quickSearch

taken to collect and protect the information and the degree to which the information is not already publicly available. In practice, the person who controls the confidentiality of the information will enjoy the commercial advantage.

In other fields such as financial services and internet and telephone service providers, this has led to calls by consumers to access "their own" information. This may also become an issue for vehicle occupants or owners who find "their" information being collected by the manufacturer or vehicle operator, as discussed in the previous chapter.

The matters covered in this chapter are just some of the intellectual property issues raised by AVs and the integration of biometrics into those vehicles. Other issues not covered include the prospect of design registration under the *Designs Act 2003 (Cth)* for new components as well as the obstacles to copyright given the thresholds for that protection to be invoked.

D. Eliminating driver fault

It is likely that the biometric technology utilized in AVs will shift the way our legal liability regimes are structured. The former Urban Infrastructure Minister Paul Fletcher has said that "Today, a lot of our liability regimes are premised on liability sitting with the driver, but in a world where the vehicle is completely in control, it doesn't make sense to attach liability to the passengers."[111] This is likely to have an impact in both the civil and criminal liability realm. Previous chapters of this white paper have examined the liability implications of AVs. In particular, we have discussed that Australia's well developed product liability law as supplemented by the imposition on certain parties (for example manufacturers) of a primary safety duty to ensure the safety of AVs can be expected to respond effectively to the introduction of this technology.

Until the transition to fully autonomous vehicle is complete, the Australian context biometrics may have a hand in improving the way in which we manage driver fatigue, particularly in the heavy vehicle industry.

Two features of modern Australia are highly relevant to the particular development of our AV scheme: mining and distance. A by-product of Australia's strong mining industry is that Australia is, as has been noted by the chief scientist, Dr Alan Finkel, "the global leader in autonomous trucks."[112] The distance between cities and regional centers also creates huge demand for long-haul freight drivers, which carries with it corresponding problems of driver fatigue.

In Australia, the current law (the Heavy Vehicle National Law, which operates in the ACT, NSW, Queensland, South Australia, Tasmania and Victoria) prescribes a minimum number of continuous hours that heavy vehicle drivers must rest in given periods of time (for instance, 7 hours continuous rest in a 24-hour period), and a maximum number of hours that can be worked in a given period (for instance, no more than 14 hours worked in a 24-hour period). Contravention

can lead to fines for the driver as well as other parties in the chain of responsibility, like the employer or scheduler. This system places the burden of fatigue management squarely on the driver and the companies or individuals that have sent the driver out onto the road.

When vehicles are fully autonomous, these fatigue laws will of course be obsolete. In the intervening period between full autonomy and the present, there is a role to be played in biometric technology that can detect the fatigue levels of the driver.

This technology will allow for the measurement of actual fatigue, whereas the hours-based system under the current law effectively acts as a proxy for fatigue, because when that law was created we lacked the technology to measure the fatigue of individual drivers. The technology, if rolled out systematically, could have the potential to capture the problem of driver fatigue in a far more precise way, and prevent the road accidents it causes. At that point it may be that we find ourselves to have outgrown the hours-based system.

111 Quoted in https://www.abc.net.au/news/2018-07-05/driverless-cars-ethical-debate-you-decide/9836786

112 Speech by the Chief Scientist Dr Alan Finkel at the Australian Road Transport Suppliers Association Global Leaders' Summit, May 8, 2018 (Melbourne Convention and Exhibition Centre). Transcript available at: <https://www.chiefscientist.gov.au/wp-content/uploads/Chief-Scientist-speech-Global-Heavy-Vehicle-Leaders-Summit-1.pdf p 3>.

V. China

Robin Li, the CEO of Baidu Inc., one of China's IT giants, recently admitted that Baidu received a ticket in July 2017 from the police because of testing a driverless car on public roads in Beijing in July 2017, which was not permitted under the traffic regulations at that time.

This regulatory vacuum soon came to an end when three government agencies in Beijing jointly issued guidelines implementing rules for road testing of self-driving cars on December 15, 2017. These were the first detailed regulations on AVs in China. Following that, Shanghai and Chongqing issued their own local regulations in February and March 2018 respectively before a national road testing guideline (the "**National Road Testing Guideline**") was finally promulgated in April 2018.

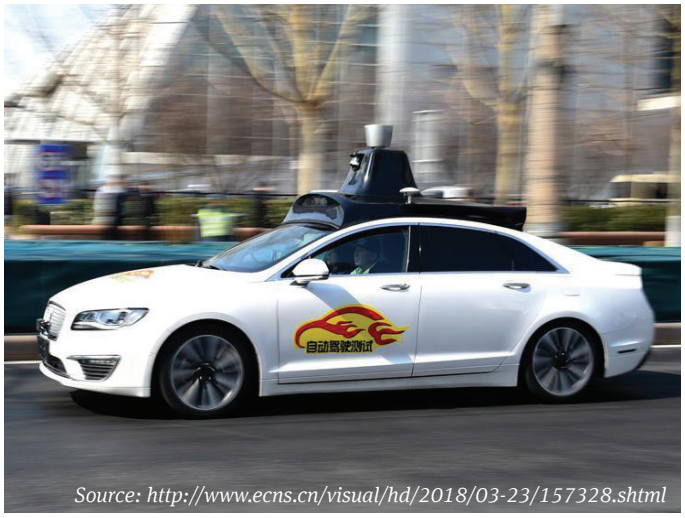
Development of intelligent vehicles can be traced back to 2015 in China, when the State Council publicized the national strategic plan *Made in China 2025* that aims to transform and upgrade China's manufacturing industry. One of the plan's priorities is to develop intelligent equipment and products, including the research and commercialization of self-driving vehicles.

Under the *Made in China 2025* plan, China saw the issuance of a number of key policies and regulations on intelligent vehicles in 2017 before the issuance of the National Road Testing Guideline.

A. National policies before the National Road Testing Guideline

Traffic matters are governed primarily by a national law, namely the *PRC Road Traffic Safety Law*, supplemented by a number of implementing rules, national guidelines and provincial or municipal regulations in China. To date, China has no comprehensive regulatory framework for AVs. While the National Road Testing Guideline has been published, it remains a subject of heated debate how self-driving cars should fit into the traditional transportation laws, product liability laws, etc.

Prior to the issuance of the National Road Testing Guideline, several policies and plans on this topic have been issued in 2017 by the State Council (the central government of China) and the primary industrial regulators, i.e. the National Development and Reform Committee ("**NDRC**") and the Ministry of Industry and Information Technology ("**MIIT**"), evidencing the government's determination to accelerate the development of intelligent vehicles at national level.



Source: http://www.ecns.cn/visual/hd/2018/03-23/157328.shtml

Barbara Li
Partner, Beijing
Tel+ 86 10 6535 3130
barbara.li@nortonrosefulbright.com

Justin Davidson
Partner, Hong Kong
Tel+ 852 3405 2426
justin.davidson@nortonrosefulbright.com

> *"The NRDC also is committed to supporting and providing financial aid to qualified projects in this sector."*

The State Council called for research on artificial intelligence and cultivation of an intelligent economy in a national plan in the middle of 2017 that encompasses development of self-driving technologies and intelligent vehicles.

Pursuant to that call, the NDRC and MIIT issued several action plans in the last quarter of 2017, including:

- the Three-Year Action Plan to Enhance the Core Competitiveness in Manufacturing Industry (2018-2020) issued by NDRC on November 27, 2017;
- the Implementation Plan for the Commercialization of Key Technologies for Intelligent Vehicles issued by NDRC on December 13, 2017;
- the Three-Year Action Plan for Bolstering the Development of the Next Generation Artificial Intelligence Industry (2018-2020), issued by MIIT on December 14, 2017;
- the Guidelines on Establishment of the National Standard System for Telematics Industry (Intelligent & Connected Vehicles) jointly issued by the MIIT and the Standardization Administration of China on December 29, 2017.

The NDRC includes intelligent vehicles as a key sector in its action plan and sets forth a number of key tasks for the commercialization of intelligent vehicle-related technologies. The NDRC also is committed to supporting and providing financial aid to qualified projects in this sector.

On the other hand, MIIT aims to establish a comprehensive system of national standards for AVs, such as terms and definitions relating to AVs, functional evaluation standards, information security standards and information perception standards. MIIT seeks to promulgate at least 30 key national standards by 2020, that will support AVs with driver assistance functions and low-level automated driving functions, and to develop a more comprehensive system with more than 100 national standards by 2025 geared to support high-level automated driving.

(i) The National Road Testing Guideline

On April 3, 2018, the MIIT, the Ministry of Public Security (the "**MPS**") and the Ministry of Transportation (the "**MOT**") jointly issued the *Administrative Rules for Road Testing of Intelligent and Connected Vehicles (for Trial Implementation)*, i.e. the National Road Testing Guideline. The National Road Testing Guideline was promulgated to introduce a nationwide legal framework for testing AVs on public roads. It took effect on May 1, 2018 and aims to facilitate the development of automated driving technology through the wide deployment of public road tests.

Key points of the National Road Testing Guideline are set out as follows:

1. Definition of Intelligent and Connected Vehicle

The National Road Testing Guideline defines the "intelligent and connected vehicle" as a new generation vehicle that is equipped with advanced car-borne sensors, controllers, actuators and other devices in combination with modern communication and network technologies, which can ultimately replace the operation by human drivers and achieve safe, efficient, comfortable and energy-saving driving. AVs should be capable of, among other things, intelligent information exchanging and sharing between the vehicle and humans, other vehicles, roads and cloud servers, perceiving complicated surrounding conditions, intelligent decision-making and collaborative control.

The automation functions of AVs are divided into three different levels, namely conditional automation, high-level automation and full automation. Conditional automation is the driving mode where the system performs all driving tasks and the driver needs to intervene when requested by the system; high-level automation is the driving mode where the system performs all driving tasks and may request the driver to respond in certain circumstances but the driver may ignore such requests; and the full automation is the driving mode where the system performs all driving tasks that a human driver can perform under all road conditions without any intervention of the driver. These are generally understood to refer to L3, L4 and L5 under the definition of levels of automation as outlined by SAE International.

2. Testing Procedures and Requirements

Before an AV can be tested on roads, a test permit (described in more detail below) must be obtained from the authority. The local counterparts of the MIIT, the MPS and the MOT at the provincial or municipal level are jointly responsible for administration of AV tests and issuance of test permits for AVs.

The following requirements must be complied with in order to obtain a test permit from the authority:

Requirements of the testing entity
The testing entity shall be an independent legal entity registered in China that has necessary technical and financial capability to, among others, manufacture vehicles and their components, conduct related research and development activities, monitor the test vehicles remotely on a real-time basis, record, analyze and reproduce an incident involving the test vehicles, compensate the losses caused by the test vehicles.

Before being permitted to test on public roads, it must complete certain tests as required by the authority in a closed test field. It shall take out traffic accident insurance with an insured amount of at least 5 million Yuan (approximately USD $750,000) or provide a letter of guarantee of the same amount for each test vehicle.

Requirements of the test vehicle
Test vehicles, including passenger vehicles and vehicles for commercial use but excluding low-speed vehicles and motorcycles, shall meet the following requirements.

First, the test vehicle should not yet be registered with the authority but must satisfy all statutory inspection and testing requirements except for endurance requirement. If any statutory testing requirement is not satisfied due to the automation function, the entity applicant must prove that the safety of the vehicle has not been jeopardized.

Second, the test vehicle shall be equipped with an autonomous driving system and have the function to switch between the autonomous driving mode and the manual driving mode safely, immediately and easily. The test driver shall be able to intervene and control the vehicle directly at any time under the autonomous driving mode.

Third, the test vehicle shall have status recording and storage as well as online monitoring functions, which enables the real-time transmission of information relating to the driving mode, the location and the movement of the vehicle, and which can automatically record specified data during the period of at least 90 seconds prior to a traffic accident or malfunction of the test vehicle and store such data for at least 3 years.

Fourth, the test vehicle must complete sufficient tests in a closed field, and its self-driving function must be tested and verified by a third-party testing institution recognized by the authorities.

Requirements of the test driver
The test driver shall have at least three years of unblemished driving experience with no record of drunk or drugged driving, no severe traffic violation record (e.g. speeding 50% over the speed limit or violation of traffic lights) for the recent one year, and no traffic accident record of causing death or serious bodily injury. It is also required that the test driver shall enter into an employment contract or a labor service contract with the testing entity. In addition, the test driver shall have a good technical understanding of the self-driving testing program and operation methods and have the capacity to deal with the emergency situations.

The testing entity shall submit relevant materials to the authority evidencing that the above requirements are complied with, and the authority will decide whether to grant a test permit in respect of each test vehicle, which will be valid for no more than 18 months. After the testing entity receives the test permit from the authority, it shall apply for a plate for the test vehicle. If any information shown on the test permit such as the testing entity, the test vehicle or the test driver is changed, the testing entity shall re-apply for a test permit.

(ii) Local rules and regulations

Local transportation authorities in Beijing, Shanghai, Chongqing, Changsha, Guangdong, Fuzhou Pingtan, Changchu, Tianjin, Zhejiang, Jinan, Wuhan and Jiangsu have promulgated local rules to further regulate AVs in their own regions:

- the *Beijing Administrative Rules on Acceleration and Promotion of Work relating to Road Testing of Autonomous Vehicles (for Trial Implementation)* issued on December 15, 2017;

- the *Shanghai Administrative Measures on Road Testing of Intelligent and Connected Vehicles (for Trial Implementation)* issued on February 27, 2018;

- the *Chongqing Administrative Rules on Road Testing of Autonomous Vehicle (for Trial Implementation)* issued on March 14, 2018.

These local rules contain similar but more detailed requirements in respect of the testing entity, the test vehicle and the test driver to the National Road Testing Guideline, with local nuances. For instance:

- The Fuzhou Pingtan rule allows an independent legal person registered in Taiwan to conduct road testing.

- Under the Changsha rule, a testing entity shall take out safety production liability insurance.

- The Chongqing rule prohibits the test driver from working for more than two consecutive hours or working for more than 6 hours per day, and a dozen local rules require the test driver to have a minimum of 50 hours' experience in operating autonomous driving system.

Applicants for road testing permits must comply with both the National Road Testing Guideline and the relevant local rules.

(iii) NDRC draft strategy

On January 5, 2018, the NDRC issued the *Strategy for Innovation and Development of Intelligent Vehicles (Draft)* ("**Draft Strategy**") for public comments, which marks a further step of the government towards its goal of promoting AVs.

The Draft Strategy envisages that by 2020, a systematic framework for China will be in place for technology innovation, industrial ecosystem, infrastructure network, regulations and standards, product regulation and information security. The Draft Strategy aims to massively develop AVs in China and sets an ambitious goal that by 2020, all new vehicles are expected to have partial or full autonomous driving capabilities and 90% of LTE-V2x, and by 2025, China hopes to have almost 100% of new vehicles as AVs, and a full regulatory regime and industry specifications are expected to be fully established and by 2035; China will become an AV superpower.

The Draft Strategy recognizes the following tasks for the development of intelligent vehicles in China:

- promoting an independent and controllable technology innovation system for intelligent vehicles;

- creating an inter-sector and integrated industrial ecosystem for intelligent vehicles;

- setting up an advanced and complete road infrastructure system for intelligent vehicles;

- formulating further regulations and standards for intelligent vehicles;

- building up a scientific and normative product regulation system for intelligent vehicles;

- building up a comprehensive and efficient information security system for intelligent vehicles.

B. Data protection and data privacy

AVs contain various sensors that are designed to collect massive data of the vehicle's operation and user's preference as well as its surroundings. The sensors generally are cameras, radar, thermal imaging devices and "LIDAR," and will collect data such as statistics, photos and videos. With the development of AVs, the concerns of data privacy and unreasonable disclosure of personal information go high.

The map for autonomous driving is a new type of electronic navigation map ("**ENM**"), and data collection, editing, processing and production of automatic driving maps can only be undertaken by an entity holding an ENM license issued by the restructured Ministry of Natural Resources of the PRC ("**MNR**"). Foreign investors are prohibited from making ENM. Where an ENM license holder cooperates with automakers in developing and testing maps for autonomous driving, the relevant surveying and mapping activities shall be conducted by the ENM license holder alone. Without the approval of the provincial branch of MNR, mapping data generated from autonomous driving technology testing or road testing (including adding contents, elements or precision to traditional ENM) shall not be provided to or shared with foreign entities or individuals or foreign-invested enterprises incorporated in China (including wholly foreign-owned enterprises and joint ventures).

China's Cybersecurity Law, which became effective as of June 1, 2017, and a series of underlying rules, regulations, guidelines and industry standards, have imposed new regulatory requirements in terms of data privacy and data protection. These new legal requirements will have significant implications for industry players in the AV industry in relation to the collection, use, processing and cross-border transfer of data. In particular:

- "Personal data" is defined as all kinds of information recorded in an electronic or other form, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including but not limited to the natural person's name, date of birth, ID number, biology-identified personal information, address and telephone number. Furthermore, "biometric data," including genes, fingerprints, voiceprints, palm prints, pinna, iris and facial recognition features, would fall within the category of "sensitive personal data."

- The collection and use of personal data must follow the principles of legality, proportionality and necessity. The data controllers shall expressly indicate the purposes, means and scope of data collection and use, and obtain prior explicit consent (rather than implied consent) from relevant sensitive personal data subjects.

- The data controllers are recommended to pseudonymize any personal data they receive.

- For the sharing and transfer of sensitive personal data, the data controllers are required to give notice to the data subjects (as to the purpose as well as the type, identity and data security capability of the data recipients), obtain the data subjects' explicit consent, and adopt security measures (e.g. encryption).

- Any personal data and critical data collected and generated during the business operation of critical information infrastructure (**"CII"**) operators within China shall be stored in China and not transferred abroad, unless any data export is made on the ground of business necessity and has passed a security assessment by competent authority, the network operators themselves or delegated third parties (as the case may be). CII covers a wide range of sectors including public communication and information services, energy, transportation, water conservancy, finance, public services and e-government, as well as "other infrastructure, that, in the event of damage thereto, loss of function thereof or leak of data therefrom, could seriously jeopardize national security, national economy or public interest of China."

C. Intellectual property

The increasing research and development in the fields of biometrics and autonomous driving has inevitably led to the birth of a lot of novel, inventive and practically applicable technologies. These technologies may be applied for and protected as patents in China under the Chinese Patent Law. The Chinese Patent Law was only first promulgated in 1984, but the Chinese patent landscape has developed rapidly over the past 35 years to support the evolution of new technologies in China.

Under the Patent Law of China, an invention, which is the subject of a patent application, must not be an existing technology, i.e. a technology known or disclosed to the public either locally or abroad. As compared with the technology existing before the date of application, an invention must have prominent substantive features and represent a notable progress, and a utility model must have substantive features and represent progress. The term of protection is twenty years for an invention patent and ten years for a utility model, counted from the date of application.

In 2017, the Guidelines for Patent Examination were amended and the requirements for claims for software-related inventions were relaxed. Accordingly, it now seems to be the case that a computer-readable medium having instructions for performing a technical method may seek patent protection. Many software innovations incorporated into AVs in China may be eligible for patent protection.

Autonomous driving

The China Patent Protection Association published the "*In-depth Analysis Report on Patents for Artificial Intelligence Technology*" in November 2018. The top five applicants for patents in the field of autonomous driving in China were named as being Baidu, Ford, Toyota, Dajiang (also known as DJI) and Beihang University. Baidu is an Internet company, which invested heavily in research and development on autonomous driving projects in recent years. Ford and Toyota are existing well-known vehicle manufacturers. DJI is a manufacturer of unmanned aerial vehicles (drones) for aerial photography and videography. Beihang is a Chinese University specialized in scientific research in this field. It can be seen that the industry players in the patents for autonomous driving are not restricted to the experienced vehicle manufacturers,

but also manufacturers of hi-tech autonomous driving devices, Internet companies which are very good at analyzing data, as well as academic or research institutes.

Since Baidu is an extensive filer for Chinese patent applications in the field of autonomous driving, it is worth studying what patent applications Baidu has filed for over the past few years. The Chinese Patent Registry published an analysis of Baidu's patent applications relating to autonomous driving on its official website in March 2018. According to the analysis, Baidu filed for its first autonomous driving-related patent in 2014, but since then the number of patent applications has increased rapidly. Baidu has filed patent applications in various technologies, with the main focus on environmental awareness (e.g. laser radar and image acquisition devices which help to detect obstacles and lane lines), operational control (e.g. switching and control of driving mode), and trial and evaluation. The report commentator was of the opinion that Baidu was relatively weak in relation to the technology of planning and decision-making and also data fusion using data gathered from multiple sensors.

Biometrics

According to a recent report published by Frost & Sullivan, biometric technology in China may be classified into six categories, namely face recognition, fingerprint recognition, vein recognition, gait recognition, iris recognition and voiceprint recognition. According to the Sullivan data, the market size for biometric identification in China has expanded steadily, and the market size in China in 2017 increased by 38.4% compared to 2016.

Face recognition technology has become more widespread in China and related technologies such as computer and optical imaging have also developed rapidly. According to the statistics published in October 2018 by the China Business Research Institute, the market size for Chinese face recognition reached RMB 2.91 billion in 2017. From 2014 to 2017, the number of patent applications for face recognition technology in China continued to increase, with an average annual growth rate of 36%. In 2017, the number of face recognition patents in China reached 2,698.

Iris recognition technology has also developed rapidly in China in recent years. According to the China Intellectual Property Right Net, Chinese applicants started to file for patents relating to iris recognition technology worldwide around the same time as applicants from South Korea, the United States and Japan. The number of worldwide patent filings by Chinese applicants was quite low in the early years, but the number of worldwide patent filings by Chinese applicants increased drastically after 2006 and has since occupied the largest portion. Among the top ten patent applicants in the global market (by volume), six of the applicants came from China. As of November 2016, it was revealed that 93% of the applicants filing patents relating to iris recognition technology in China were domiciled in China. These Chinese applicants are mainly research institutes and enterprises in Beijing, including China Institute of Automation, Chinese Academy of Sciences, China University of Science and Technology, Beijing Tiancheng Shengye Technology Co., Ltd and Beijing Zhongke Hongba Technology Co., Ltd, etc. This record of patent applications shows that shows that Chinese corporations are keen to develop biometrics technology and are aware of the benefits of seeking patent protection not only in the domestic market but also globally.

> *"By 2025, China hopes to have almost 100% of new vehicles as autonomous vehicles."*

Integration of biometrics to autonomous driving

Sullivan suggested that there is a trend of integrating different biometric technologies rather than relying on a single biometric technology in order to improve security. For example, Chinese manufacturers have integrated palm and palm veins, fingerprints and faces into the same identification. The use of multiple biometrics technology can achieve better recognition performance and reliability than a single biometrics technology, increase the difficulty of forging human biometric features and improve product safety. Nevertheless, composite biometrics technology is not a simple additive integration between biometrics, and it is necessary to develop new algorithms based on the characteristics of different biometrics to achieve geometrical improvements in computational efficiency and accuracy. Similarly, it is not surprising to see how biometric technology will be integrated to the field of autonomous driving for the convenience of the public.

There appears to be little overlapping to date between the key players in the fields of biometrics and autonomous driving. It is anticipated that different companies will cooperate and obtain the right to use other biometric or autonomous driving technologies through licensing or acquiring other technology companies. There are provisions restricting the import and export of technologies in China. A Chinese citizen or legal entity which grants a license or assigns its patent to a foreign company will be subject to the Regulations of Administration of Import and Export of Technology in China. For example, the import and/or export of technologies may be restricted in order to protect the public interest or enable acceleration of development of certain industries locally. It remains to be seen how different entities will cooperate in order to integrate these technologies.

D. Challenges to insurance industry

General auto insurance regime in China will apply to AVs, but no doubt the widespread adoption of AVs will have a great impact on the automobile insurance industry. For example, insurance costs are expected to shift from the individual car owners to the automobile manufacturers gradually because the automakers will likely be held accountable for accidents occurred during the self-driving mode. Insurance premiums will drop considerably, since accidents will decrease as human drivers will make fewer mistakes with the assistance of the automated system. Commercialization of artificial intelligence and big data technologies and mass production of AVs in the near future will have far-reaching consequences for insurance businesses in China. Currently, however, given the early stage of the development and testing of AVs, it has been provided in the National Road Testing Guideline that an AV testing entity must take out traffic accident insurance with an insured amount of at least 5 million Yuan (approximately USD $750,000) or provide a letter of guarantee of the same amount for each test vehicle.

E. Conclusion

Recent developments in the sector are welcomed by the industry and clearly show China's determination and commitment to bolster the AV sector. The national and local road testing guidelines and rules represent a firm step towards an upgraded and intelligent automobile industry. It is expected that more regulations and national standards will be promulgated shortly. Testing permits for AVs have been granted to large Chinese and international automotive and tech companies, such as Alibaba, Baidu, Tencent, Shanghai Automotive, BMW, etc., in multiple cities in China in 2018, and we expect more testing permits will be issued. Interaction between new technologies and traditional laws may present both opportunities and challenges for the industry players and they should keep a close eye on future developments.

VI. France

According to a study led by Deloitte in 2019, French consumers are more confident than other Europeans about AVs: only 36% of French people say they are skeptical about them in 2019 (vs. 65% in 2017) compared to an average of 50% for other Europeans, who believe that such vehicles are not yet sufficiently safe.[113] Identically, French consumers are less worried about the collection and the sharing of their biometric data by connected vehicles than elsewhere in Europe. Finally, 34% of them trust original equipment manufacturers in the role of data manager when it comes to their personal data, rather than others (government, car dealerships, insurance companies, cloud service providers, etc.). These perceptions are reflected in the French regulations governing biometrics as well as the associated laws relating to this type of data.

A. Legal and regulatory framework

In France, the experimentation of AVs is subject to the issuance of a prior administrative authorization pursuant to the Energy Transition Act in 2015[114] and the government order relating to the testing of "vehicles with delegated driving authority" in 2016.[115] The authorization is valid for two years (renewable once). A decree adopted in 2018[116] provides that such authorization can only be granted for one of the three following purposes: tests to develop key technologies for AV (software, sensors, mapping, etc.) or connected road infrastructure, evaluation of performance in real-life situations for future uses, and public demonstration in order to raise public and companies' awareness. The decree lays down a number of security and information obligations to be complied with. Regarding data, the data collected must be regularly erased (except in the event of an accident, where the data collected five minutes before the accident must be kept for one year).

From the end of 2014 to the beginning of April 2018, 54 authorizations were issued. Alongside the big car manufacturers (such as Renault, PSA), small companies have emerged in the sector: Navya has launched its "Autonom shuttle" in 2015, currently tested in closed circuits (notably in hospitals, airports and in the ski resort Val Thorens), and an "Autonom cab" tested in Lyon. Created in 2014, Easymile introduced last year TractEasy, a "luggage tractor" currently tested in a PSA factory. Public transport operators such as RATP, Keolis and Transdev have also launched trials, aiming at facilitating transportation in public spaces.

The French legal and regulatory framework on AVs is still evolving, and two pieces of legislation are expected in 2019. Firstly, the Action Plan for business growth and transformation ("*PACTE*" law) will supplement the 2015 Act by making any type of trial possible, including those without a person in the vehicle. Secondly, the Law on Mobility ("*Loi des mobilités*") should establish a framework for the definitive system of AV traffic.

112 Deloitte, European global automotive consumer study 2019.
114 Act No. 2015-992 of August 17, 2015 on the energy transition for green growth.
115 Ordinance No. 2016-1057 of August 3, 2016 on the testing of delegated driving vehicles on public roads.
116 Decree No. 2018-211 of March 28, 2018 on the testing of vehicles with delegated driving authority on public roads.

Nadège Martin
Partner, Paris
Tel+ 33 1 56 59 53 74
nadege.martin@nortonrosefulbright.com

Cécile Auvieux
Associate, Paris
Tel+ 33 1 56 59 53 93
cecile.auvieux@nortonrosefulbright.com

(i) Autonomous vehicles and personal data

The collection and processing of personal data through AVs is subject, like any other processing of personal data, to the European General Data Protection Regulation 2016/689 ("GDPR")[117] and its supplementing national laws, such as in France, the French Data Protection Act as amended.[118]

The French data protection authority (the CNIL) published a compliance package on "connected vehicles and personal data" in 2017[119], which already took into account to some extent GDPR requirements. While this package does not addresses all of the specific privacy issues which will be faced with AVs, it still constitutes a first step towards the definition of standards for all stakeholders of the connected car industry. At the international level, the International Working Group on Data Protection in Telecommunications (IWGDPT), adopted on April 9 and 10, 2018, a Working Paper on Connected Vehicles.[120]

All are encouraging the car industry to favor connected vehicles involving local personal data processing with no data transmission to service providers or car manufacturers (scenario IN-IN[121]). This scenario has the advantages of both providing car users with safeguards of their privacy and simplifying the obligations for data controllers, as it implies that the data must necessarily be processed and stored inside the vehicle.

According to the CNIL, processing falling under that IN-IN scenario (i.e. no personal data transmitted to the service provider and users retaining full control over their data) can benefit from the "household exemption" provided by Article 2.2.c of the GDPR, i.e. they are considered as processing carried out by a natural person in the course of a purely personal or household activity and therefore not subject to data protection laws.

However, with AVs, the exchange of data will hardly be limited to the confines of the car itself. AVs will need to interact and communicate data with other vehicles, traffic systems, etc., in real time, and the legal implications and compliance with privacy laws of these data usages and flows will have to be reassessed in that particular context.

Please refer to Norton Rose Fulbright's third annual Autonomous Vehicle White Paper for further information on the use of personal data in autonomous/connected vehicles in France.

B. Processing biometrics in autonomous/ connected vehicles

(i) French legal and regulatory framework for processing biometrics

Biometric data qualify as "special categories of personal data" within the meaning of GDPR and the French Data Protection Act. Unlike other personal data, they are inherent in the human body, can be communicated unconsciously and, in most cases, cannot be modified. These characteristics are why, as a sensitive data, their processing is prohibited, except in a limited number of circumstances laid down in the GDPR, among which are the data subject's express consent or the protection of the data subject's vital interests.

In France, an additional derogation has been introduced in the French Data Protection Act. Article 8.II.9° authorizes the use of biometrics by employers for purposes of access control by biometric authentication to the premises, computer devices and applications in the workplace, if such processing is compliant with the Model Regulation recently adopted by the CNIL.[122]

The CNIL has also released several guidelines on the processing of individuals' or customers' biometrics, notably in relation to smartphones[123] or daily life activities.[124] The CNIL insists on limiting the risks associated with biometric processing while guaranteeing that people using them control their personal data and its recommendations incorporate data protection principles from the design stage and by default.

(ii) Biometrics in the automotive industry

No guidance relating to the processing of biometrics applied to AVs specifically has been released yet. However, the CNIL addressed the issue in relation with connected vehicles, in its compliance package mentioned above. Note that this package applies to the private use of connected cars and excludes as such the employer/employee context.

117 Regulation (EU) 2016/679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
118 Law n° 78-17 of January 6, 1978 relating to IT, files and liberties.
119 CNIL, "Compliance pack: Connected vehicles and personal data", October 17, 2017.
120 See press release; https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2018/20181004-PM-Arbeitspapier_zu_vernetzten_Fahrzeugen-en.pdf
121 See Norton Rose Fulbright's third annual Autonomous Vehicle White Paper (France chapter).
122 Deliberation No. 2019-001 of January 10, 2019 on the Model Regulation relating to the implementation of devices aimed at access control by biometric authentication to the premises, computer devices and applications in the workplace.
123 CNIL, "Biometrics in personal smartphones: application of the data protection framework," July 24, 2018.
124 CNIL, "Biometrics made available to individuals: what are the principles to be observed?" April 10, 2018.

The following requirements or best practices expected by the CNIL can be inferred from the analysis of this compliance package (being specified that these same requirements can be found in all other guidance released by the CNIL in relation to the processing of biometric data).

Local processing and local storage. The processing shall ideally be carried out at the initiative and under the control of the data subject and for private use, provided that the biometric data is stored inside the device, in a locked environment and in an encrypted way, and during the access control, only one chip or piece of data indicating the success or failure of the biometric recognition is transmitted. It means that no biometrics data shall be transmitted to the service provider or the car manufacturer. However, they remain the controller of the data processing implemented, and specifically of the security (e.g. by limiting the possible number of authentication trials). It also means that the driver or car user shall be able to deactivate the biometric authentication device at any time, and easily access or delete the history of biometric data (via, for example, a button inside the vehicle and/or via his computer or on-board computer).

Consent and alternative. In order to unlock, start and activate certain vehicle controls through the biometric data of the driver or car user, the CNIL considers that consent shall be the legal ground. Consent is the legal ground when an individual wishes to unlock or start a vehicle thanks to a fingerprint, activate some of the vehicle controls through recognition voice or be alerted in case of drowsiness through recognition of pressure points exerted by the back of the driver or car user in the front seat. Such processing implies full control by the user over his biometric data and can only be based on consent. The requirement for full control includes that an alternative shall always be offered to the user of the biometric device.

The data subject must be provided with clear information on the biometric device and its alternative and can choose the alternative without any additional constraints or incentives. Moreover, the data subject's agreement shall be specific to the biometric authentication, and not diluted in larger terms and conditions (or a larger privacy policy).

Security measures. Biometrics data are highly sensitive data, and the CNIL requires the implementation of strict security measures, in addition to the "classic" security measures that shall be implemented in connected vehicles, in order to ensure that the authentication device is safe and reliable enough. It is therefore recommended to ensure that:

- the setting of the biometric solution used (for example, false positive and false negative rates) is adapted to the expected level of security for access control;
- the biometric solution used is based on a sensor resistant to the attacks that are deemed trivial in the state of the art (such as, currently, the use of a flat-printed print for fingerprint recognition);
- the number of authentication attempts is limited;
- only the biometric template is stored in the device, in an encrypted form using a cryptographic algorithm and key management that comply with the state of the art;
- the raw data used to create the biometric template and for user authentication are processed in real time without being stored locally (for example, audio recordings in the case of a voice-recognition system).

If the processing meets such requirements regarding local storage and processing, consent and alternative and specific security measures, it falls under the "household exemption" and is therefore not subject to the laws and regulations relating to the protection of personal data.

Any other processing is subject to the GDPR and the French laws and regulations on personal data, and specifically on biometrics. In this event, the car manufacturer or the service provider accessing the biometric data shall document how they comply with the applicable laws and regulations (e.g. if consent is not obtained, they shall justify why the use of biometrics is strictly necessary). A data protection impact assessment may be necessary.

Employee/employer context. Note that if the biometric device were to be used in an employee's vehicle, it will have to be assessed whether the device at hand would fall within the scope of the CNIL's Model Regulation on the use of biometrics by employers for access purposes to tools or applications made available at work, and as such, would have to strictly comply with all the requirements of that Model Regulation. In particular, the employer would have to justify the strict necessity of the use of biometrics in that particular context.

VII. Germany

The German government and the European Commission have declared biometric technologies to be key enablers for a digital economy with a multitude of potential fields of application to recognize, authenticate and identify persons based on physical and/or behavioral characteristics.[125] The market agrees: The biometrics market is growing rapidly since investors increasingly recognize the potential of biometrics and related technology. Biometric technology is a small but important building block to ramp up investments into self-driving vehicles and will also help to make assisted driving safer during the transition period (e.g. by sleep detection systems). For that reason biometric technology companies are attractive targets for strategic and financial investors in the automotive sector.

The application fields of biometric technology are numerous: biometrics can be used in verification processes for vehicle entry and engine start; they enable surveillance of the driver’s and passengers’ vital functions including connected health care services; they can also be used for individual and automatic comfort and ambience settings that can be automatically adjusted on the basis of biometric data generated from the passengers in the vehicle (car personalization); they may also be used by insurers in identification processes for telematics as well as by service providers for in-vehicle payments.[126] All biometric technologies have in common that they work with pattern matching methods. For the development of effective pattern recognition systems vast amounts of data samples and references are required. Complying with data protection and privacy laws is of paramount importance in biometrics. In 2017 the German Federal Ministry of Transport and Digital Infrastructure

124 European Commission, Digital Transformation Monitor, Biometrics technologies: a key enabler for future digital services, January 2018, page 2.

126 Cf. Allianz, A brave new world: Vehicle biometrics, pages 2 et seq.

Frank Henkel
Partner, Munich
Tel+ 49 89 212148 456
frank.henkel@nortonrosefulbright.com

Christoph Ritzer
Partner, Frankfurt
Tel+ 49 69 505096 241
christoph.ritzer@nortonrosefulbright.com

Eva-Maria Barbosa
Partner, Munich
Tel+ 49 89 212148 461
eva-maria.barbosa@nortonrosefulbright.com

Christina Lorenz
Senior Associate, Munich
Tel+ 49 89 212148 342
christina.lorenz@nortonrosefulbright.com

Tiffany Zilliox
Senior Associate, Munich
Tel+ 49 89 212148 364
tiffany.zilliox@nortonrosefulbright.com

Alexander Mathes
Associate, Munich
Tel+ 49 89 212148 419
alexander.mathes@nortonrosefulbright.com

published ethical guidelines on connected and AVs which mainly addressed data privacy and transparency issues.[127]

In the following, we will explore the major legal implications and specific areas of interest in connection with biometric technology and AVs in Germany.

A. Mergers & acquisitions

(i) General M&A trends in the automotive technology sector

The M&A landscape is highly driven by innovation and emerging technologies.[128] Technology driven investments are constantly growing in all sectors and have increased by 60% since 2015.[129] The Autotech sector has also seen significant growth over the past years.[130] Traditional vehicle makers and other companies in the automotive sector acquire or build partnerships with innovative technology startups and established technology companies to proactively embrace current trends in the ever-changing automotive market environment.[131] The goal is to integrate intelligent technologies into the vehicles to connect them, make them smart and finally autonomous. Not surprisingly, sensors, radar and LIDAR, as well as software aimed at the processing and analysis of large data amounts, have become particular drivers for M&A activity in the automotive sector. In addition, with disruption in the automotive industry progressing rapidly, a significant number of M&A transactions is paving the way for the current products of many automotive manufacturers being transformed into service offerings of future mobility services providers.

While market data evidence that the deal volumes for M&A in mobility services have reached unprecedented levels (particularly through a number of megadeals in car sharing and ride hailing), the average deal volume of investments in autonomous driving technology has declined — while at the same time the number of deals, as well as the number of majority participations acquired by investors, has increased. This trend is a sign for more early-stage investments in autonomous driving technology as well as an increase in strategic investments.[132]

127 German Federal Ministry of Transport and Digital Infrastructure, Ethics Commission – Automated and Connected Driving – Report (Extract), June 2017.
128 Cf. PwC Deals . Global Automotive M&A Deals Insights Year-end 2016, page 1; PwC Deals – Global Automotive Deals Insights Year-end 2018, page 1.
129 EY, Technology driven M&A in the automotive industry – From automobile to autonomous, 2018, page 6.
130 PwC Deals – Global Automotive Deals Insights Year-end 2018, page 5; Thomson Reuters – Uncertainty and Risk in the Global Automotive Industry, 2018, page 4.
131 EY, Technology driven M&A in the automotive industry – From automobile to autonomous, 2018, page 3.
132 Cf. EY, Technology driven M&A in the automotive industry – From automobile to autonomous, 2018, page 6.

(ii). Investing in biometrics

M&A activities in the biometrics sector have many things in common with M&A activities in traditional technology sectors. Lessons learned from M&A in the biometrics sector highlight in particular the necessity to pursue a well-considered, holistic due diligence approach for a buyer to successfully complete an acquisition – be it in bilateral transactions or in transactions in from of an auction process.

Understanding the target company's current economic and financial state of play as well as its technological offerings is of core importance for an investment to prosper. Investments concerning cutting-edge technologies such as biometrics require a potential buyer to ascertain at the earliest possible moment the technical sanity of the biometric technology to be acquired. Such technology assessment should be embedded in a thorough legal and financial due diligence – including, in particular, anticipating the future application cases for the respective biometric technology. To avoid siloed information, potential buyers have found it extremely helpful to have the legal due diligence include a legal technology consultancy element – which Norton Rose Fulbright provides, for instance, through its very own technology consultancy practice. The involvement of the technology consultancy practice can help to bridge the gap between the technical and legal assessment of an investment in biometrics – sometimes drilling down to legal and technical issues arising on the level of the coding and the programming of the software itself. Biometric technology used in the context of autonomous driving combines statistical methods with biometric data collected through vehicles and stationary infrastructure.[133] For that reason, the legal due diligence needs to focus specifically on the compliance with data privacy laws as well as on the often challenging copyright and IP related issues. It is also essential to identify cyber risks and evaluate the effectiveness of countermeasures in connection with the use of biometrics in AVs. Legal issues may also arise from competition regulation as well as product liability and tort laws.

In the current competitive market environment, the time frame for such a holistic approach to due diligence in the course of an M&A transaction is often very tight. This narrow window frames the need for a potential buyer not to waste time and to instruct and involve qualified legal advisors already at an early stage in the M&A transaction. At such early stage, additional focus should be placed on the suitable acquisition structure, not only from a tax but also from a corporate governance perspective.

133 Federal Government Office for Science, Biometrics - A guide, 2019, page 1.

As far as the latter is concerned, the specific requirements may differ on a case-by-case basis. Strategic investors may seek to implement governance structures that allow them to integrate the target company fully into an existing corporate structure in order to benefit most from synergies within the own business ecosystem. Financial investors will often abstain from taking direct operational decisions – but will entrench their financial interests and exit expectations through various rights and instruments on the level of the rules of procedure, the articles of association and the investment agreement. The earlier such respective governance requirements are identified and articulated by a potential buyer, the less friction and delay will be experienced at later stages in the transaction timeline.

B. Data protection and security

An AV is typically recording and processing personal data, including *inter alia* biometric characteristics that could be considered biometric data under the EU privacy laws. The car is equipped with many sensors that record the driver (as long there is still one and the car has not reached level 5 with full autonomy) and the vehicle's surroundings. Biometrics could be used to identify and authenticate the driver or car owner before unlocking the car, initiating the ride or detecting signs of sleepiness or drunkenness for safety purposes. This may happen with fingerprints, facial or behavioral recognition techniques – as already known by modern smartphones. The advantage is that these means of identification and authentication are easy to use and seem to be more secure. Regarding the vehicle's surroundings, typically sensors and cameras scan public streets to allow the vehicle to predict and avoid possible accidents. Such recordings may be used live during the ride, to steer the vehicle, or may be recorded and transmitted to the operator to allow the artificial intelligence (AI) behind the AV to learn from new traffic situations and optimize the algorithms used. Theoretically, such recordings could also allow the operator to use face recognition techniques to re-identify traffic participants in different situations, allowing the AI to better predict their future behavior in traffic.

Art. 4 (14) GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic data." According to this definition, only biometric characteristics that result from specific technical processing and could permit the unique identification of a person would be considered biometric data.

> *"To avoid siloed information, potential buyers have found it extremely helpful to have the legal due diligence include a legal technology consultancy element..."*

As automated vehicles use specific technical processing, the first requirement is easily met. Such data as age, height and gender are generally not considered biometric data under the GDPR, as they do not usually allow the unique identification of a person according to the Conference of the Data Protection Authorities in Germany (*Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder*)[134]. According to the German Data Protection Authorities, biometric samples, i.e. the analogue or digital representations of biometric characteristics prior to biometric characteristic extraction, as well as biometric characteristics, i.e. the numbers or distinctive features extracted from a biometric sample and that can be used for comparison purposes, could be classified as biometric data under the GDPR[135].

Based on this definition, not all biometric characteristics used in automated vehicles can be regarded as biometric data. In particular, the information pertaining to bodily characteristics used to identify and verify the vehicle owner or driver, such as fingerprints and facial recognition, are clearly biometric data. The behavioral data used to control the vehicle falls under the definition only if it enables unique identification of the person. For example, the driver's behavioral information generally indicating sleepiness or drunkenness would not be considered biometric data within the scope of the definition.

Biometrics is one of the "special categories of personal data" under Art 9 GDPR that broadly prohibits the processing of biometric data for the purpose of uniquely identifying a natural person, but it recognizes certain legal bases to justify

134 Position paper on biometric analysis adopted on April 3, 2019 p. 19 available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/DSK-Positionspapier-zur-biometrischen-Analyse.pdf

135 See above p. 20

its processing, chiefly, the explicit consent of the data subject, the performance of specific contracts or processing for certain specific purposes.

When the data relates to the driver or the vehicle's owner, a solution to use his/her sensitive or biometric data could be an explicit consent. According to the German Data Protection Authorities the consent must explicitly refer to the use of the biometric data.[136] Therefore, there must be an explicit reference to the biometric data and its sensitivity in the consent. The German Data Protection Authorities stated in the Hambach Declaration on Artificial Intelligence[137] that decisions (e.g. identification and verification) based on the use of AI systems must be transparent and comprehensible. It is not sufficient to provide an explanation with regard to the result; the data subject must also be able to understand the processes. Moreover, the algorithms involved must also be sufficiently explained.

Furthermore, the specific purpose of the data processing needs to be stated, e.g. unambiguous identification of the vehicle's owner.[138] Further, the EU privacy laws require such consent to be freely given. An operator of the service, therefore, cannot require the user/driver to necessarily give such consent. Practically, that means that the operator has to offer alternatives as to how the users/drivers can identify or authenticate themselves – so that the biometrics use is an option that only the individual can freely decide to use or not.

The information collected from the vehicle's surrounding are not necessarily considered as biometric data or even personal data. If the vehicle only recognizes that the people (e.g. children) are on the road, such data does not allow individual identification of the data subject and therefore does not fall under the definition. If a unique identification could be possible, it would be more difficult to find a legal ground for processing of such biometric data. Typically it is not possible to receive consent from each person on the street. None of the other grounds under Art. 9 GDPR are easily applicable. Alternatively, the operator may argue that optimizing AI algorithms are a form of research and might therefore rely on the GDPR's research exemptions. This is a tricky path, however, which might be available during development, but less easy in the later regular operation of the service.

Finally, the operator of the AV service would have to consider that biometric data require special technical and organizational measures that must be adequate to the risk exposure of such data. Biometric data especially is very demanding to secure – an attacker who misuses the fingerprint or facial recognition is a nightmare. Once this data is in public, how should the affected "owner" of the data react? He cannot just change his face or thumb like he would be able to change a password or user login. The damages that might occur by disclosing and misusing biometric data probably can never be fully mitigated again. The principal concern of the Article 29 Working Party, an advisory body made up of a representative from the EU data protection authorities (**"WP29"**) replaced by the European Data Protection Board, is the security and confidentiality of biometric data in order to prevent unlawful use. In this respect the WP 29 has made recommendations. The German Data Protection Authorities have not yet developed guidelines and recommendations on technical and organizational measures to implement a biometric authentication, and the development of such measures is the responsibility of industry and science.[139]

Following the recommendation of the WP29, service providers should generally avoid storing such data in the cloud, but only in a secure place in the vehicle itself. If the data is stored in the cloud, the data controller has to establish a detailed policy on how to control its contractors, such as unexpected inspections, and require guarantees regarding employees, procedures regarding individual's rights, etc.[140] Further, the entire fingerprint should not be saved, but only single reference points, allowing the right user to identify when the thumb is presented, but not allowing a third party to misuse such reference points only.

C. Biometrics and insurance

The use of biometric data may bring significant advantages to the insurance industry. However, it remains to be seen to what extent the following will actually occur, due to restrictions by data protection law (e.g. special protection of biometric data for the purpose of uniquely identifying a natural person and of data concerning health as special categories of personal data).[141]

136 See above p. 22
137 Hambach Declaration on Artificial Intelligence issued by the German Data Protection Authorities, dated April 3/4 2019 available at https://www.datenschutz-bayern.de/dsbk-ent/DSK_97-Hambacher_Erklaerung.html
138 See above footnote 1, p. 20
139 See above footnote 4.
140 Working paper 193 on developments in biometric technologies adopted by the WP29 on April 27, 2018, p. 13 available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf
141 See Art. 4 no. 14 and 15 as well as Art. 9 General Data Protection Regulation 2016/679.

(i) More tailored insurance programs

With the use of biometric data and the availability of ever more accurate data comes the chance for more focused underwriting decisions and more sophisticated tailoring of insurance programs. Insurers already make use of voluntary self-tracking data as a basis for the premium calculation.[142] Such data are currently available from telematics products ("Pay how you drive" (PHYD) and "Pay as you drive" (PAYD)). While "Pay how you drive" only relates to vehicles with drivers "Pay as you drive" also relates to AVs. In Germany "Pay how you drive" products are offered by several insurers.[143]

The use of biometric data, in conjunction with telematics, enables a very thorough representation of the insured risk by building a more personal picture of the driver.[144] While "Pay as you drive" is tailored in a static way to an individual vehicle with a fixed number of drivers, insurance programs for AVs may be tailored to an individual policyholder in a dynamic usage based way. In particular, this makes it possible to tailor the insurance program to the frequency of use of a certain vehicle by a certain driver, which can be monitored due to respective technology. This personal picture of the driver is especially useful when a policyholder uses several vehicles (e.g. car sharing). Biometrics technology and data can also integrate further value-added services such as user authentication and camera systems directed at the driver to detect fatigue or drowsiness, resulting in alerts.[145] Insurers may bind such value-added services as an option to existing auto insurance.[146]

Biometric data being available is expected to have a positive impact on underwriting and determination of the insurance premium.[147] Biometric data also creates an opportunity for insurers to provide more personalized insurance policies with flexible insurance rates specific to drivers.[148] This driver-specific insurance is currently already discussed for highly automated vehicles where a reduction of the premium might be considered by an insurer if a policyholder often allows the automated systems to take over instead of driving himself.[149]

(ii) Claims handling

Use of biometric data is expected to have an impact with regard to claims handling relating to AV accidents. AVs are already generally expected to be involved in fewer accidents than vehicles with drivers, even though such accidents will be more expensive due to highly sophisticated in-vehicle systems, including biometrics technology. In addition to this general advantage of AVs, more accurate data being available, such as driver identification data, will likely decrease the amount of fraudulent claims.[150] If biometric data can be used by claims handlers in real-time this would speed up the claims process even further.

(iii) Cybersecurity

Since AVs are connected to the infrastructure and services, and are becoming more and more like IT machines, their vulnerability to possible cyber attacks and the need for cybersecurity increases accordingly. There continues to be concern that hackers might intentionally cause accidents or perpetrate theft of AVs. While recognition systems (e.g. fingerprint or smartwatch) or monitoring by geolocation services may decrease the risk of the vehicle being stolen,[151] a risk remains that the security might be bypassed even if the technology and software is constantly updated and further developed. In order to mitigate the risks for safety, security and data privacy insurers may, for example, insist that different biometrics modalities[152] multi-factor authentication identifying an authorized driver might be installed in the car for accessing the car and starting the engine. Insurers of cyber risks will also consider which technology is used to reduce the risk of cyber attacks on databases store biometric data and how potential consequences are mitigated. With regard to fingerprints there

142 Schmidt-Kasparek, *More and more motor insurers with telematics tariffs* (Apr. 11, 2019), https://rp-online.de/wirtschaft/immer-mehr-autoversicherer-mit-telematik-tarifen_aid-38051291; Allianz, *Less expensive insurance tariffs for Autonomous Vehicles* (Sept. 12, 2017), https://www.handelsblatt.com/finanzen/banken-versicherungen/allianz-guenstigere-kfz-tarife-fuer-autonomes-fahren/20314616.html?ticket=ST-42973-zfexoTx95iytnXSo2X4J-ap6.

143 Wilkens, Heise Online, *Bosch intends to teach learning to autonomous vehicles* (Mar. 16, 2017, https://www.heise.de/newsticker/meldung/Bosch-will-selbstfahrende-Autos-das-Lernen-lehren-3655412.html referring e.g. to a joint development by HUK Coburg and Bosch of a "Pay how you drive."

144 Allianz Insurance plc, *A brave new world: Vehicle biometrics* (Sept. 28, 2017), https://www.allianzebroker.co.uk/news-and-insight/news/a-brave-new-world-vehicle-biometrics.html.

145 Vieweg, Sueddeutsche Zeitung, *Driver, please identify yourself* (Mar. 17, 2015), https://www.sueddeutsche.de/auto/bessere-wegfahrsperren-fahrer-gib-dich-zu-erkennen-1.2389270.

146 European Commission, Digital Transformation Monitor, *Biometrics technologies: a key enabler for future digital services* (Jan. 2019).

147 Similar with regard to data from wearable technology: Hauari, Digital Insurance, News, *Biometrics on the rise as insurers look for smoother experience*, interviewing e.g. M. Taht, MunichRe (August 1, 2017).

148 European Commission, Digital Tranformation Monitor, *Biometrics technologies: a key enabler for future digital services* (Jan. 2019).

149 Allianz, *Less expensive insurance tariffs for Autonomous Vehicles* (Sept. 12, 2017), https://www.handelsblatt.com/finanzen/banken-versicherungen/allianz-guenstigere-kfz-tarife-fuer-autonomes-fahren/20314616.html?ticket=ST-94305-zmyNwFyqRAtoPuqdQaod-ap6.

150 Allianz Insurance plc, *A brave new world: Vehicle biometrics* (Sept. 28, 2017), https://www.allianzebroker.co.uk/news-and-insight/news/a-brave-new-world-vehicle-biometrics.html.

151 Vieweg, Sueddeutsche Zeitung, *Driver, please identify yourself; VW and BMW count on biometrics for prevention of theft* (Mar. 17, 2015), https://www.sueddeutsche.de/auto/bessere-wegfahrsperren-fahrer-gib-dich-zu-erkennen-1.2389270; Editors, Autoreparaturen.de, Biometrics: How your vehicle recognizes you (Jan. 12, 2017), https://www.autoreparaturen.de/blog/allgemein/biometrie-wie-dich-dein-auto-erkennt.html.

152 See Goode Intelligence, White Paper, *Biometrics for the Connected Car* (Dec. 2017), https://www.goodeintelligence.com.

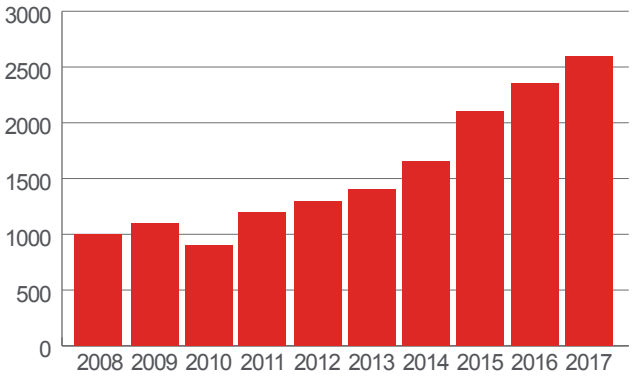
is, for example, already technology available which ensures that even if the database is hacked only algorithms are available and not pictures of the fingerprint, to ensure that hacked data cannot be used for identification purposes.[153]

D. Patent landscape – analysis for Germany and Europe

(i) Development of the autonomous driving patent landscape in Germany

Over the last years, the numbers of patent applications and granted patents in the autonomous driving sector have significantly increased in Germany. According to an analysis conducted in February 2018 by the German Patent and Trademark Office (DPMA), the number of patent applications in Germany regarding autonomous driving increased from around 1,000 applications in the year 2008 to far more than 2,500 applications in the year 2017.[154] This development of the total patent application numbers in the field of autonomous driving per year is demonstrated in the following chart.

Patent applications for Germany



Notably, the patent applications regarding autonomous driving started to rise substantially and steadily from the year 2012 onwards. The patent applications for Germany which are included in these figures are national patent applications and PCT applications in the national phase. The analysis conducted by the DPMA was based on a selection of several relevant IPC classes. The IPC is an international system which subdivides the whole sector of technology into classes ordered in a hierarchical structure, so that all patent documents worldwide can be assigned to certain fields of technology. For the mentioned analysis, the DPMA identified the IPC classes which are related to autonomous driving. This group includes IPC classes as to autonomous driving course control, assistance systems for drive control, traffic control, vehicle electronics in general, navigation, sensor technology and environment sensor systems. Unfortunately, none of the IPC classes deals exclusively with autonomous driving. The problem therefore is that a clear distinction from other technical areas is not possible. There is no generally valid definition which would allow the integral and conclusive assignment of patent documents to the field of AVs. Thus, an analysis based on IPC classes is rather a more or less accurate approximation to the current status of patents regarding autonomous driving. The same is true for the even more specific field of biometrics technology in the field of autonomous driving (see further below). Notwithstanding, a clear upwards trend is visible for patent applications in the IPC classes relevant to autonomous driving according to the DPMA figures.

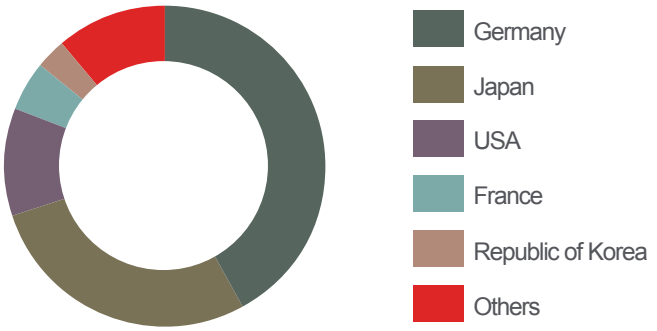
The DPMA also assessed the nationality of the patent holders, in order to identify the origin of the increasing numbers of patent applications. The DPMA analyzed the patents that are valid and in effect in Germany until the end of the year 2017, including German national patents granted by the DPMA and European patents granted by the European Patent Office (EPO). The top patent holders with most patents granted with effect in Germany in 2017 are national but also international companies. The top three are Audi AG, Toyota Jidosha K.K. and Volkswagen AG. Notably, the largest amount of patents is owned by German entities, i.e. 42% share of all patents considered. The second largest group of patent holders is from

153 DPA, CIO, *The challenges of biometrics* (Apr. 25, 2019), https://www.cio.de/a/die-herausforderungen-der-biometrie,3597159Dpa, Handelsblatt, *Devices with identification for by biometrics, New biometrics sensors promise enhanced security for smart phone and tablet* (Mar. 12, 2019), https://www.handelsblatt.com/technik/it-internet/biometrische-geraeteauthentifizierung-neue-biosensoren-versprechen-mehr-sicherheit-fuer-smartphone-und-tablet/24087914.html?ticket=ST-8143-fnJ3cDWssy93vdUNgXQj-ap6.

154 Analysis and publication by the Federal Patent and Trademark Office regarding patents in the field of autonomous vehicles: https://www.dpma.de/english/our_office/publications/background/autonomousdriving/autonomousdrivingpart3/index.html. The figures, tables and charts in this section are based on the publication of the DPMA analysis.

Japan, with a large 28% share. Followed by US patent holders with only 11% of shares, as well as patent holders from France, the Republic of Korea and further states. The following chart and the respective table represent the situation in 2017:

Patents valid in Germany at the end of 2017



Patents valid in Germany at the end of 2017[1]

Country[2]	Number
Germany	2,006
Japan	1,350
USA	527
France	227
Republic of Korea	150
Others	550
Sum	4,810

[1]patents granted by the German Patent and Trade Mark Office and the European Patent Office; EP patents at the DPMA after publication
[2]country of the first patent holder at the end of 2017

Among the German patent holders, the following companies were identified to be the top holders of autonomous driving patents:

Top patent holders from Germany[1]

Top 10	Holder[2]	Number
1	Robert Bosch GmbH	480
2	AUDI AG	321
3	VOLKSWAGEN AG	203
4	Bayerische Motoren Werke AG	130
5	Continental Automotive GmbH	93
6	Harman Becker Automotive Systems GmbH	71
7	Deutsches Zentrum für Luft- und Raumfahrt e.V.	44
8	Continental Teves AG & Co. oHG	42
9	Valeo Schalter und Sensoren GmbH	36
10	Daimler AG	33
11	Robert Bosch Automotive Steering GmbH	33

[1]country of the first patent holder at the end of 2017
[2]first patent holder at the end of 2017; possible interlinking of business enterprises was not taken into consideration

The German car manufacturers Audi AG and Volkswagen AG are ranking among the top three patent holders. However, in the German market they are dominated by Robert Bosch GmbH with more than double the number of patents of VW AG. Among the top patent holders also listed are the German car manufacturers BMW AG and Daimler AG, but with significantly fewer patents.

(ii) Biometrics patents for automobile and autonomous driving in Germany and Europe

The advantages of the use of biometric modalities in automobiles are recognized more and more by the automobile manufactures and OEMs. Starting from the demand for better protection against car thefts, along with measuring the body dimensions of the driver[155] for adapting and optimizing the configuration of the driver cabin, up to monitoring the attention of the driver,[156] a huge amount of different fields of use of biometric systems in automobiles is available and conceivable.

The IPC class system has, as a matter of principle, no specific classes for biometrics, neither with regard to their particular use in automobiles nor in AVs. As explained above, the consequence is that an analysis on the basis of IPC classes does not guarantee a full and exhaustive picture of the patent activity, but it nevertheless allows to identification of certain overall industry trends. For this purpose, we conducted an analysis of the European patent applications for three exemplary IPC classes which have a relation to biometrics in automobiles and AVs, and noticed a clear upwards trend in the time period from 2008 to 2018.

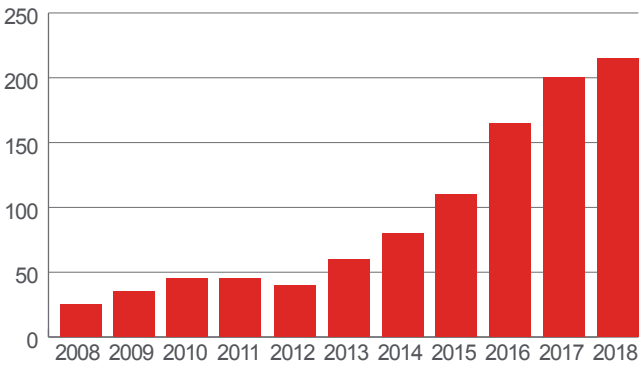
Notably, one exception to the general rule is the specific IPC class concerning “fittings or systems for preventing or indicating use or theft of vehicles by using biometry” (IPC class B60R 25/25). This IPC class has a very particular scope regarding locking systems for vehicles by using biometry. Therefore the number of European patents applied for is quite low. Since 2008 only around 40 European patent applications were published or European patents granted. It is noteworthy that the patent applicants for this kind of patents are mainly automobile manufacturers and automobile equipment suppliers. Among the applicants, for example are German and international automobile manufacturers Volkswagen AG, Audi AG, Toyota Co Ltd., Jaguar Land Rover Ltd and Ford Motor Company Group. Furthermore, automobile supplier Robert Bosch GmbH, as well as international suppliers, like the French Valeo Group, have filed such patent applications.

Beyond this specific IPC class, all technical inventions using biometrics, even though they are not specifically claimed for application in automobiles, are usually also fit for use in AVs. For example, if the patent protects an invention relating to a heartbeat scan, the respective invention may not only be used within a sports watch, but also for stopping an automobile in case of a detected heart attack of the driver. Therefore, the analysis of biometrics usable in automobiles or AVs must be extended to a further patent class regarding “security arrangements for protecting computers, or components thereof, (...) against unauthorized activity by using biometric data, e.g. fingerprints, iris scans or voiceprints” (IPC class G06F 21/32).

What is striking when reviewing the list of applicants for this category of patents is that these essentially include companies from the electronics industry. Overall, the number of published European patent applications and the granted patents in the time period from 2008 to 2018 amount to nearly 1000 documents. Significantly, the top three applicants are Samsung Electronics Co. Ltd., Fujitsu Ltd. and Intel Corp. Surprisingly, the automobile manufacturers are totally absent from the list of applicants for this patent class.

In general, the patenting activity shows an increasing focus on biometric systems for automobiles and AVs in the past years, as can be seen from the following chart depicting the numbers of the granted European patents and European patent applications for the IPC classes G06F 21/32 and B60R 25/25:

Granted EP and published EP applications



155 https://www.autozeitung.de/nissan-gesaesssensor-biometrisch-fahrer-analyse-qashqai-ab-april-76185.html#
156 https://www.elektroniknet.de/elektronik-automotive/assistenzsysteme/fahrerueberwachungssystem-fuer-teilautonomes-fahren-im-ct6-157484.html

Obviously, the numbers of European patent applications and grants for this field of growing interest has increased dramatically since 2013.

The same trend can be observed with similar patent categories. For example the IPC class covering "methods or arrangements for reading or recognizing printed or written characters or for recognizing patterns, e.g. fingerprints" (IPC class G06K 9/00) may also be relevant for biometrics in automobiles. An exemplary patent application for the IPC class G06K 9/00 is a method for identifying an individual by recognizing the eye position of the respective individual by a camera, which is protected by a European patent application (EP 3 158 499) filed by Robert Bosch GmbH. The number of granted European patents and published patent applications in the IPC class G06K 9/00 has significantly increased over the last ten years. Starting from year 2008 with nearly 400 patents and patent applications, the number per year has steadily increased to reach triple that amount with over 1200 patents and patent applications in 2018. The ranking of granted patents and published patent applications over the last 10 years in this category is again predominantly led by international electronics companies like Samsung Electronics Co. Ltd., Fujitsu Ltd. and Sony Corp., as well as software and telecommunication companies such as Microsoft or Qualcomm Inc. Nevertheless, automobile manufactures and automobile suppliers are active in this field and still hold a certain number of granted patents and published patent applications. Among the top applicants are, for example, Honda Motor Co. Ltd, Toyota Motor Co. Ltd., Saab AB and Nissan Motor. The German company Audi AG has been granted and filed 34 patents in the last 10 years. Bosch GmbH, as the world's largest automobile supplier, holds 105 patents and patent applications for the IPC class G06K 9/00 in the analyzed time period between 2008 and 2018.

With the growing importance of the technologies of biometrics in automobiles and autonomous driving, various established companies from different backgrounds, in both automobile and non-automobile sectors, as well as specialized startups are getting more and more active and emerging in the market.

Yet, when comparing the patenting strategy of several leading companies established in the US, it seems that their focus lies in the US market rather than in Europe. Comparing the overall patent numbers, it appears that some of the leading US entities are not proactively applying for patents in the member states of Europe. For example, specialized startup companies like Veniam Inc., Digimarc, Intelligent Technologies International Inc., Z Advanced Computing Inc., Nio USA Inc. and SmartDrive Inc., with a particular focus on essential AVs technology, do not yet seem to seek to cover the European market. The respective companies have roughly 440 issued patents and pending patent applications in the US, whereas in the EU the total number solely amounts to 70.

> *"Thus, it is likely that the risks of future patent enforcement and patent litigation regarding biometrics systems in autonomous vehicles will be increasing for the automobile manufacturers."*

Taking a closer look at Veniam Inc. as the leading company in the specific field of biometrics in AVs, the divergent numbers are striking. Veniam Inc. filed 16 US patent applications and currently owns 67 US patents in the respective field. However, in the European Union, Veniam Inc.'s only activity over the last 10 years was the filing of 10 patent applications at the European Patent Office in the year 2018. Digimarc, as one of the most active of the abovementioned companies, applied for nearly 40 patents in the European Union, but the gap to the US with around 190 patent applications is still significant.

Furthermore, start-up companies like Intelligent Technologies International Inc., Z Advanced Computing Inc. and Nio USA Inc. did not appear to have any noticeable activity on the European patent landscape over the past years, unlike in the US In view of these findings, one may wonder about the reasons for these discrepancies and whether the strategies followed by these companies specialized in AV technology are not focusing on the importance of the European market.

The same is true for non-practicing entity Liberty Peak Ventures LLC and American Vehicular Sciences LLC which have not yet established a patent portfolio for the European market.

Considering that the market for biometrics technology in autonomous driving systems is determined by the presence of various players from extremely different backgrounds - ranging from automobile manufacturers, their suppliers and specialized startups to worldwide operating electronics, telecommunication and software companies - a change of the automobile industry as it existed is inevitable. Thus, it is likely that the risks of future patent enforcement and patent litigation regarding biometrics systems in AVs will be increasing for the automobile manufacturers.

VIII. Indonesia

A. Regulatory framework

As in the case with the operation of **AVs**, there is no specific regulatory framework for the uses of biometrics either for general use or specifically for the integration of biometrics into AVs in Indonesia. The absence of regulation, however, does not necessarily mean that Indonesia does not recognize the uses of biometrics.

The Government of Indonesia has implemented biometrics technology in the new electronic residential card (Kartu Tanda Penduduk Elektronik – **eKTP**) which was introduced in 2009. The eKTP uses biometrics in the form of automated fingerprint identification system to recognize the individual Indonesian resident. Under Law No. 24 of 2013 on the Amendment of Law No. 23 of 2006 on Residential Administration (**Residential Administration Law**), we note that the biometrics in the forms of fingerprint and retina data of the Indonesian resident are classified as 'personal data' and shall be stored by the government of Indonesia. The Residential Administration Law, however, does not set out whether the requirement to classify biometrics as personal data and to store the biometrics in Indonesia also applies to other uses of biometrics, including its uses in AVs or other devices (such as phones, computers, etc).

B. Biometrics privacy and cybersecurity issues

(i) Data privacy

Biometrics is a technology which uses human physiological and behavioral characteristics. The unique human physiological and behavioral characteristics are what will be considered as 'personal data'[157], and on the assumption that the AVs developer will obtain the biometrics data through electronic measures, several requirements under the Minister of Communication and Informatics (**MOCI**) Regulation No. 20 of 2016 regarding Protection of Personal Data in an Electronic System (MOCI 20/2016) shall apply.

Under MOCI 20/2016, several requirements for AV developers who wish to collect personal data through electronic measures are, among others:

a. to obtain certification for its electronic system;

b. to have an internal policy on the protection of personal data;

c. to obtain consent for collecting, processing, analysing, storing, disclosing, transfer and deletion of personal data by providing a written consent form, either manually or electronically, using the Indonesian language;[158] and

d. to only use, process, disclose and share the personal data in accordance with the given consent.

(ii) Storing, sharing and transferring personal data

With respect to the storing of biometrics which are classified as personal data, there is a possibility that the government of Indonesia will argue that the biometrics must be stored in Indonesia in accordance with the requirement of the Residential Administration Law. The requirement to store the biometrics data onshore will be a different approach from the current rule which regulates that personal data for private uses (such as for integration of biometrics into AVs) can be stored overseas.[159] If this is the case, the AV developers may be required to have data storage facilities in Indonesia.

157 Indonesia currently does not have any specific law which covers a broader range of personal data protection. The current prevailing regulation only regulates personal data protection in the context of an electronic system – i.e. Minister of Communication and Informatics (MOCI) Regulation No. 20 of 2016 regarding Protection of Personal Data in Electronic System (MOCI 20/2016). MOCI 20/2016 defines personal data as true and actual in an individual data which is attached and can be identified either directly or indirectly to certain individual.

158 It is possible in practice to provide the written consent form in bilingual.

159 It is important to note that pursuant to Law No. 11 of 2008 on Electronic Information and Transaction (as amended) (EIT Law) and Government Regulation No. 82 of 2012 (GR 82/2012), the obligation to set-up data center in Indonesia applies to "public service" electronic system providers. Unfortunately, there is no definition provided in the above mentioned law and regulation on the meaning of 'public service'.

Benny Bernarto
Partner, Jakarta
Tel+ 62 21 2965 1802
benny.bernarto@nortonrosefulbright.com

Tias Karina
Associate, Jakarta
Tel+ 62 21 2965 1829
tias.karina@nortonrosefulbright.com

If the AV developers are required to have an onshore data center, it is important to note that the existing regulations are silent as to whether the relevant AV developers should own the data center or could outsource/subcontract the onshore data center. In practice, electronic system providers in Indonesia (for public services and non-public services) can cooperate with a third party data center provider on a contractual basis in order to provide such onshore data storage.

If the AV developers are allowed to store the biometrics data offshore, note that storing such biometrics personal data offshore may be considered as offshore transfer of personal data which would trigger further requirements under MOCI 20/2016.[160] Notification of this offshore transfer of personal data must also be given to the customer/data owners, and the AV developers must also obtain consent from the customer/data owners prior to the offshore transfer of personal data. Similarly, as in the event of breach of other personal data, the AV developers are required to provide written notification to the customer/data owners within 14 days of the failure.

(iii)Cybersecurity

The absence of regulatory framework on biometrics does not mean that crimes related to biometrics are not regulated. The Residential Administration Law sets out several sanctions related to the manipulation or illegal disclosure of residential data (including biometrics data) – which sanctions include imprisonment of two to six years and fines of IDR 25 million to 75 million. Additionally, Law No. 11 of 2008 as amended by Law No. 19 of 2016 regarding Electronic Information and Transaction (**ITE Law**) has covered a broad range of sanctions applicable to crimes related to electronic systems such as hacking, illegal distribution/transmission, illegal access and interception of electronic system and data – which will apply to biometrics use as well. Under the ITE Law, any hacking, illegal distribution/transmission, illegal access and interception are subject to imprisonment of 4 to 12 years and fines of IDR 600 million to IDR 10 billion.

In case the cybersecurity related to biometrics affects the safety of AV road transportation, note that sanctions under Law No. 22 of 2009 on Road Traffic and Transportation may also be imposed to the AV developers – such as in the forms of suspension or revocation of license to operate in Indonesia.

(iv) Intellectual property

Integration of biometrics to the operation of AVs requires protection of intellectual property related to the technology and devices used to collect the biometrics. In this case, it is likely that one intellectual property aspect which must be protected is patent.

With respect to patent, Indonesia adopts the principle of "first registration" and requires that any patent must be registered in the Indonesian Patent Registry. However, since Indonesia has ratified the Paris Convention for the Protection of Industrial Property, the patent holder in its country of origin (subject to whether the country of origin is a party to the Paris Convention for the Protection of Industrial Property) will reserve priority rights to be registered first in the Indonesian Patent Registry, and Indonesia will acknowledge the patent registration date of an invention in its country of origin.

One potential issue with becoming a patent holder in Indonesia is that Law No. 13 of 2016 on Patent (Patent Law) requires the patent holder to manufacture or process its product in Indonesia in order to support the transfer of technology, encourage investment and/or increase work opportunity. Patent Law (including in the previous regime of Patent Law) does not set out sanctions for noncompliance with this requirement, but the Patent Law provides a mechanism for any party have a national interest (including a prosecutor) to submit a claim to the commercial court for revocation of patent if the patent holder fails to manufacture or process its product in Indonesia. This provision has given rise to many protests from various stakeholders including governments from several countries.

The government of Indonesia then issued Minister of Law and Human Rights Regulation No. 15 of 2018 on Implementation of Patent (MOLHR Reg 15/2018) which allows the patent holder to submit application to delay its obligation to manufacture or process its product in Indonesia, however, for a period of only 5 years, with possibility of an extension. This application must be submitted to the Minister of Law and Human Rights no later than 3 years as of the date of the patent.

160 MOCI 20/2016 requires that any offshore transfer of personal data must be made after coordinating with the MOCI, in which the coordination will be on case by case basis by way of (i) submission of plan; (ii) discussion; and (iii) submission of implementation report.

C. Conclusion

In the absence of relevant regulations, it appears that the growth and uses of biometric in Indonesia, in particular in the private sectors such as banks and financial institutions, outpace the regulation. For examples, a domestic bank has introduced voice biometrics as part of its customer authentication protocol while a Japanese firm has also launched a payment service using fingerprint authentication in Indonesia. It is understood globally that many of the major auto manufacturers are currently in various stages of research and development on AVs, either independently or in partnership with technology companies. However, it also appears that most of the patents and patent applications relating primarily to biometrics in AVs belong to technology or independent automotive research and development companies that are deeply invested in developing AVs and related technologies, including the incorporation of biometrics, and not the automotive manufacturers. The automotive manufacturers should carefully consider the obligations under the data privacy regulations, in particular with respect to the possible requirement to maintain the data in Indonesia and the division of responsibilities between the automotive manufacturers and the technology companies with respect to the data protection. Care should also be taken with respect to the use of the technology in relation to its patent and the obligation under the Patent Law for a patent holder to manufacture or process its product in Indonesia. With respect to the Indonesian market, it would be the interest of the automotive manufacturers to have an understanding on whether the biometrics technology that being used in the automotive vehicles is or will be a registered patent in Indonesia.

"The automotive manufacturers should carefully consider the obligations under the data privacy regulations, in particular with respect to the possible requirement to maintain the data in Indonesia, and the division of responsibilities between the automotive manufacturers and the technology companies with respect to the data protection."

IX. South Korea

Korea has seen an increasing use of biometrics in vehicles and related electronic products. As an illustration, Samsung’s Galaxy mobile phones enable the user to unlock the phone by face recognition and Hyundai’s new Santa Fe vehicles enable the driver to unlock and start the car using his/her fingerprint.

Under Korean law, a person’s biometric data is considered personal data, the use of which is governed most notably by the Personal Information Protection Act (the **“PIPA”**) and the Promotion of Information Communications Network Utilization and Personal Information Protection Act (the **“Network Act”**).

In December 2017, the Korea Communications Commission and Korea Internet & Security Agency jointly published a guideline on the protection of biometric information. This guideline is not independent legislation specifically regulating the use of biometrics, but it is considered the relevant authorities’ confirmation that biometrics constitute personal information under Korean law and their guidance on how biometrics should be used and protected under the current data protection laws of Korea.

Thus, to understand the current regulatory framework for use of biometrics in Korea, it is essential to understand Korea’s laws on personal data protection, which already impose specific and strict obligations on those who collect and use a person’s biometrics.

A. Personal data protection laws

The ground rule when collecting personal data is that only the minimum amount of personal data necessary for the intended purpose should be collected. Some additional key rules include obtaining prior consent from the data subject for the collection and use of personal data, taking proper measures to prevent the loss, theft or leakage of the personal data, and destroying personal data without delay when it is no longer needed.

B. Personal data

In Korea, personal data is broadly defined. Personal data means information pertaining to a living individual, which contains information identifying a specific person by name, national identification number, visual image, and so forth. Personal data also includes information that by itself cannot be used to identify a specific person but that enables the easy identification of such person if combined with other information.

Under Korea’s data protection laws, biometrics include physiological and/or behavioral characteristics that facilitate the identification or authentication of individuals (e.g. use of fingerprint and facial recognition to unlock vehicles). If such characteristics are not used for identification or authentication of individuals (e.g. simple recognition of approximate age

Tehyok Daniel Yi
Sr. Foreign Counsel, Yulchon LLC
Tel+ 82 2 528 5512
thyi@yulchon.com

Kyu Sang Hwang
Partner, Yulchon LLC
Tel+ 82 2 528 5635
kshwang@yulchon.com

Sun Hee Kim
Partner, Yulchon LLC
Tel+ 82 2 528 5838
kimsh@yulchon.com

Seo Young Lee
Associate, Yulchon LLC
Tel+ 82 2 528 5175
seoyounglee@yulchon.com

or gender to transmit targeted advertisement), they are not considered to be the data which is protected by Korea's data protection laws.

C. Prior consent required for collection of personal data

Data collection requires prior consent of the data subject, after having been notified in advance of the following matters: (i) purposes of collection and use of the personal data; (ii) items of personal data to be collected; (iii) period of time for which the personal data will be held and used; and (iv) data subject's right to withhold his/her consent and disadvantages that may result by withholding consent.

In addition, collection and use of special types of personal data – including "sensitive information" which may seriously infringe upon the privacy of the individuals, such as information regarding political opinions, health and genetic information, and "uniquely identifying information" such as a resident registration number and passport number – requires a separate opt-in consent.

The consent form itself is heavily regulated in Korea – with specific rules for font size and checkboxes, for example.

D. Transfer of personal data

Any transfer of personal data to a third party for such third party's own use, in which the third party recipient obtains the personal data for its own benefit and business, also requires prior consent of the data subject. Here, transfer of personal data to a third party for such third party's own use should be distinguished from an entrustment of personal data to a third party, in which the third party recipient obtains personal data for the purpose of performing work entrusted by the original data collector, and the original data collector has the obligation to monitor, supervise and educate the third party recipient, regarding the protection of the entrusted personal data. In the event of any violation of personal data protection laws, there is also a divergence. The original data collector would be liable for any breach committed by the third party to whom personal data is entrusted, but not for the actions of a third party to whom personal data has been transferred for the third party's own use.

Transferring personal data abroad (i.e., to a foreign entity) also requires the data subject's consent in advance after notifying matters prescribed by law.

E. Management of personal data and security measures

Certain technical, administrative, and physical measures must be implemented to protect personal data from loss, theft, leakage, alteration or damage. Such measures include the encryption of personal data and maintaining safe storage facilities with appropriate locking devices.

In connection with the obligation to take security measures for the protection of personal data, both the PIPA and the Network Act promote cybersecurity through imposing certain duties to prevent unauthorized access to the network system (e.g. firewall, password system and network segregation) and analyze the cause of any intrusion into a network system and to take measures in response.

F. Penalties

A violation of Korea's personal data protection laws could lead to criminal liability and administrative fines, as well as exposure to civil lawsuits. For example, a person who collects personal information without consent may be punished by imprisonment for not more than 5 years or by a fine not exceeding 50 million Korean won (approx. USD 43,000), and an administrative fine of up to 3% of the annual sales for the relevant business under the Network Act. Additionally, failure to implement data security measures that results in data loss, theft, leakage, alteration or damage may be punished by imprisonment for not more than 2 years or by a fine not exceeding 20 million Korean won (approx. USD 17,000), and an administrative fine of up to 3% of the annual sales for the relevant business under the Network Act.

G. Other rules governing biometric data

In consideration of the heavy regulations governing the collection and use of personal data, which also apply to biometrics, the following rules are particularly worth noting.

First, biometrics may be considered to be "sensitive information" under the PIPA, which will require a separate opt-in consent for its collection and processing.

Second, when applying the rule on data minimization – i.e., only the minimum amount of personal data necessary for the intended purpose should be collected – care should be taken to destroy without delay the original biometrics once they are converted into the biometric identifiers and safely encrypted. Otherwise, consent must be obtained for its continued retention and use. Also related to the rule on data minimization, the data controller and processor should ensure

that sensitive data should not be unnecessarily extracted from the original biometrics (e.g. ethnic data, religion or health information).

Third, the data subjects should be given various methods to easily control the use of biometrics (e.g. by using a cellphone or website). The data controller and processor is advised to offer alternative identification or authentication methods (e.g. passwords), that may be used in case the users withdraw their consent to use their biometrics or become unable to use the biometrics due to changes in their physical or behavioral traits.

Lastly, biometrics should be securely protected from theft and unauthorized use. In particular, biometrics should be encrypted using a secure algorithm when being stored or transmitted through a network.

H. Conclusion

Could the restrictive personal data protection laws impede the widespread incorporation of biometrics into AVs in Korea?

In the US, for example, the strong protections imposed by Illinois' law on the collection of biometric data – requiring written individual consent and allowing a private right of action against private entities for violations – have deterred some companies from offering the use of their biometric technologies to consumers in Illinois.[161]

In Korea, strong personal data protection laws may give rise to concerns that may similarly dissuade companies from using biometrics. Nevertheless, Korea-based companies, such as Samsung and Hyundai, have already heavily invested in biometrics technologies. In addition, to reduce the impediments created by the strong personal data protection laws, various members of Korea's National Assembly have sought to amend the PIPA and the Network Act. It is therefore possible that the great commercial potential of biometrics and AVs may stem changes to Korea's personal data protection laws and their interpretation and application.

> *"The consent form itself is heavily regulated in Korea — with specific rules for font size and checkboxes, for example."*

161 Please see pages 13-14 of the US chapter.

X. Turkey

Turkey has been following global trends in adaptation of biometrics in technology, particularly in identification and security technologies. As of 2018, Turkey has a population of 82.4 million.[162] 96% of the population own a mobile phone,[163] 41.9 million of which are smartphone users.[164] In big cities like Istanbul and Ankara, security systems such as hand geometry recognition, iris or fingerprint scans are widely used to enter office buildings, new residential complexes and even luxury gyms. Mobile service providers, banks and insurance companies use voice recognition to authorize their customers access to their accounts. Another example of voice recognition is voice command technologies used in recently released cars that Turkey imports from other countries.

However, despite using biometrics in different contexts from touchID of smart phones to voice recognition for paying internet bills, collection, storage, processing and destruction of biometric data was not regulated by a privacy law in Turkey until 2016. The law that entered into force in 2016 originates from the European Union Directive 95/46/EC; however, certain areas still remain untested or are yet to be clarified by lawmakers.

A. Biometrics and data protection regulations

In Turkey, the main regulation governing the protection of personally identifiable information is the Law No. 6698 on the Protection of Personal Data (the "Data Protection Law") that came into effect on April 7, 2016. Before, it was not clear how biometric data could be stored and processed under Turkish law. The Council of State ruled on several occasions that since privacy is a constitutional right, and storing and using biometric data is a limitation of the right to privacy, such a waiver can only be granted by a duly enacted law. In fact, the Council of State declared face recognition and fingerprint recognition practices in public buildings unconstitutional due to breach of privacy before the Data Protection Law was introduced. Therefore, the entry into force of the Data Protection Law was a milestone in the regulation of biometrics in Turkey, as it introduced the long-awaited regulatory framework for protection of biometric data.

Under the Turkish data protection regime, personal data may not be processed without the data subject's explicit consent. Biometrics are defined as sensitive data under the Data Protection Law and are subject to the rules applicable to protection of sensitive personal data. Biometric data may only be processed without the data subject's explicit consent if it is for the purposes of the protection of public health, the provision of preventive medicine, medical diagnosis, treatment and care services or the financial planning and management of healthcare services. Data that falls within one of these exceptions may only be processed by persons or authorized institutions bound by the duty of confidentiality.

161 Turkish Statistical Institute, 2018 Population Statistics.
162 "Turkish Heritage." *Technology - Turkish Heritage Organization*, www.turkheritage.org/en/issues/technology.
163 "Smartphone Users in Turkey 2017-2023 | Statistic." *Statista*, www.statista.com/statistics/467181/forecast-of-smartphone-users-in-turkey/.

Lale Tuzmen
Foreign Legal Advisor, New York
Tel+1 212 318 5305
lale.tuzmen@nortonrosefulbright.com

B. Transfer of data rules

As a rule, personal data may not be transferred outside of Turkey without the data owner's explicit consent. Nevertheless, the law provides an exception for certain types of data when sufficient protection is provided in the foreign country where the data is to be transferred, or the data controllers in Turkey and in the related foreign country sign a written undertaking guaranteeing sufficient protection and the Board has authorizes the transfer. Health data falls within one of these exceptions and can be transferred outside of Turkey if the recipient country provides sufficient safeguards. The Data Protection Agency ("DPA") has still not published the list of countries where sufficient data protection safeguards are provided. Therefore, in practice, in order to transfer data outside of Turkey, the data controllers in Turkey and in the recipient country should sign a written undertaking to guarantee sufficient safeguards and obtain DPA's approval. The DPA's approval will take into consideration the reciprocity of data transfer to Turkey from the country where data is intended to be transferred.

C. Uses of biometrics

(i) New biometric ID cards and drivers' licenses

In 2016, the laws relating to Civil Registration Services was amended[165] to the effect that national ID cards would store biometric data and that this data may not be used for purposes other than identification. Unfortunately, what the biometric data would entail was not defined until 2017 when the same law was amended again. Accordingly, biometric data to be stored on national ID cards was defined as: "Personal data obtained from fingerprint, vein trace and palm taken to ensure the identification and authentication process through electronic systems."[166]

Similarly, Turkey also switched to new drivers' licenses with an electronic chip in 2016, which would hold data relating to the holder's fingerprints and blood type. The deadline for changing existing drivers' licenses with a new one is 2021.

> *"As a rule, personal data may not be transferred outside of Turkey without the data owner's explicit consent."*

(ii) Banking regulations

Turkish Banking Regulation and Supervision Agency has published rules on information systems security.[167] Accordingly, the ID verification mechanism applied to customers should be composed of at least two different components independent from each other; data points that are "known" by the customer, "owned" by the customer or "which are a biometric characteristic" of the customer. For the element "known" by the customer, components such as password/changeable password may be used, for the element "owned" by the customer, a changeable password producing device or a changeable password procured by SMS service may be used. The components shall be entirely special to the customer and the ID verification shall not be realized and the services shall not be accessed without presenting those components.

This communiqué was amended and the definition of biometric data was added in 2010 as follows: "Biometrics means the unique human physiological and behavioral characteristics that are measurable and attributable to that person." This rule is the legal basis for the voice recognition systems used by banks for their customer service hotlines.

165 Law No. 6611 on Amending the Military Service Law and Certain Other Laws dated January 14, 2016 published in the Official Gazette No. 29606 dated January 27, 2016.

166 Law No. 5490 on Civil Registration Services dated April 25, 2006, published in the Official Gazette No. 26153 dated April 29, 2006.

167 Communiqué on Principles to be Considered in Information Systems Management in Banks, published in the Official Gazette No. 26643 dated September 14, 2007.

(iii) Employment law

Under Turkish labor law, employers are required to keep a file for each employee.[168] This file must include all relevant information and documents required by law, in addition to personal information. The employer must submit the file to the appropriate public authorities for inspection whenever asked. However, the employer is obliged to maintain the files in a lawful manner with utmost good faith and not to disclose any information which the employee might have a legitimate interest in keeping confidential.

Employers are also required to ensure that their employees receive data protection training. There should be disciplinary sanctions if the employees act against the data protection policies and procedures of the company.

(iv) Races and games

Another interesting use of biometrics for security reasons was recently introduced in 2018 with an amendment to the Horse Races Regulation. Accordingly, registering a horse for a derby now requires biometric identification of the horse owner or an authorized representative through face recognition, fingerprint recognition, palm veins recognition, etc.

On the other hand, the new electronic card system called "Passolig" which replaced all printed tickets for soccer games does not use any of the biometric recognition systems that are becoming widely used in other countries' stadiums.

(v) Biometrics regulations and autonomous vehicles

The laws that regulate the highways and the traffic do not yet include provisions relating to AVs or biometrics. Therefore, the general rules applicable to protection of biometrics would apply to biometric data collected within the context of AVs. Due to the unanswered questions on protection of sensitive data (for example, to which countries sensitive data can be sent), and the likelihood of additional legislation in the future, automobile manufacturers as well as importers should be careful to consider privacy requirements to avoid data-breach fines. If, for example, gait and gesture recognition data collected in Turkey is stored in a data center outside of Turkey, data controllers should comply with the data privacy requirements related to cross-border data transfer.

D. Consequences of non-compliance

Data may not be processed without the explicit consent of the data subject, except as explicitly listed under the legislation. Also, data must be collected for a specific and legitimate purpose, be relevant and not disproportionate to the purpose of processing, and be processed in accordance with the general principles set by the law.

In case of an unauthorized destruction of, disclosure of, or access to personal data, the subject may either follow the specific breach notification and complaint procedures under the data protection laws or may resort to other remedies provided under Turkish criminal law as explained below.

Turkish Criminal Code provides criminal sanctions for violations in relation to the use of personal data. Criminal acts regulated under the Turkish Criminal Code directly relating to the use of personal data are as follows:

i. Violation of privacy (Article 134)

ii. Unlawful recording of personal data (Article 135)

iii. Unlawful access to or disclosure of personal data (Article 136)

iv. Failure to destroy any data subject to destruction as per relevant laws (Article 138)

Unlawful collection of personal data with respect to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sexual life or health conditions is an aggravating condition.

If the above criminal acts are committed by legal entities, specific security measures will apply, such as revocation of privileges, disgorgement of lost profits, or confiscation of property used for unlawful purposes.

The default jurisdiction rule is that Turkish laws apply to criminal offences committed within the Turkish territory (including its airspace and territorial waters). In addition, under specific circumstances, Turkish law may apply even if the criminal offence has been committed outside of Turkey.

168 Labor Law No. 4857 dated May 22, 2003 published in the Official Gazette No. 25134 dated June 10, 2003.

Accordingly, criminal offences committed by a Turkish citizen or a foreigner may be subject to Turkish laws, if they are (i) one of the special category crimes listed under the Turkish Criminal Code (e.g. crimes against the security of the state, constitutional order, national defence, relations with foreign states) or (ii) punishable by imprisonment of at least one year and upon fulfilment of additional conditions.

Offenders of breach of privacy and unlawful collection of personal data laws might be subject to one to three years of imprisonment, while unlawful access to or disclosure of personal data is punishable by two to four years of imprisonment. Commission of these offences by a public official misusing his/her position or by benefiting from convenience offered by a profession or trade, are aggravating conditions.

E. Conclusion

Biometric technologies are increasingly becoming a part of daily life, from completing banking transactions to entering office buildings. Data privacy is a new area of law with some untested grounds and unanswered questions, such as the list of countries that are safe to transfer the data collected in Turkey. It is likely that the regulators will provide more guidelines as the new technologies evolve. In the meantime, car manufacturers should pay attention to the biometric data that they collect and make sure to treat it as sensitive personal data.

> *"If the above criminal acts are committed by legal entities, specific security measures will apply, such as revocation of privileges, disgorgement of lost profits, or confiscation of property used for unlawful purposes."*

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

NORTON ROSE FULBRIGHT