MARCH 2018

AUTONOMOUS VEHICLE ENGINEERING™

Big Data, Big Challenges

Managing the mountain of data required for safe automated-vehicle operation

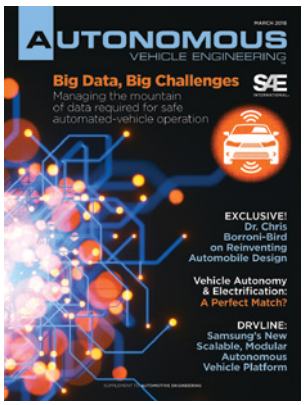
EXCLUSIVE!
Dr. Chris Borroni-Bird on Reinventing Automobile Design

Vehicle Autonomy & Electrification: A Perfect Match?

DRVLINE: Samsung's New Scalable, Modular Autonomous Vehicle Platform

SUPPLEMENT TO **AUTOMOTIVE ENGINEERING**

Contents



On the Cover

A single automated vehicle will generate its own cosmos of data—every day. Who will collect it? Who decides who gets to see and use it? Will it ever be truly private? (images: iStock)

Bioprivacy: Designing for a Moving Target

It's no secret that autonomous vehicles will assimilate massive amounts of data—including biometric information about occupants. Engineers and developers need to design systems to help assure bioprivacy.

by Jennifer Dukarski

Automotive design standards and specifications can be moving targets. In the autonomous realm, the present lack of formal rulemaking and applicable new Federal Motor Vehicle Safety Standards, coupled with emerging industry standards, requires a designer to remain nimble. Building on these technologies to incorporate biometrics into vehicles, yet another moving target emerges: bioprivacy rights.

Autonomous vehicles will expand harvesting of biometric data

Biometric data generally refers to any medical or physiological data relating to a person. A biometric "identifier" offers the ability to trace unique physiological data to a specific individual and includes fingerprints, facial or retinal scans and genetic profiles. Biometric identifiers are lucrative targets for the automotive industry: Goode Intelligence projects the market for automotive-related biometric content may reach a value of $969 million by 2023.

As designers of driverless vehicles focus on the user experience (UX), the following applications become the data collectors for biometric identifiers:

- **Eyes on the road—a disengagement solution system:** A potential solution to determine the driver's ability to return to control after autonomous operation.
- **Personalization and safety:** Driver-identification technology can use facial and iris scans, as well as voice and fingerprint tracking.
- **A healthy and entertaining UX:** A touch of a holographic button or the shift of an eye could allow a user to access a personal cloud-based movie or music playlist.

Protection under federal law: is it applicable?

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) required the creation of standards for the electronic exchange, privacy and security of health information. In response, the Privacy Rule was released and applied to covered entities (health plans, healthcare clearinghouses or healthcare providers that transmit health information) and their partners (known as business associates). Under the regulations, covered entities and business associates must take additional actions to protect health information they collect, store or transmit.

There often is confusion in the application of HIPAA to biometric data and identifiers collected by a vehicle. Unless that data is collected by or involves a covered entity, HIPAA and the Privacy Rule do not apply.

A fast-changing realm: state law protections for biometric identifiers

In the absence of comprehensive federal bioprivacy legislation, state data-protection laws have emerged. While varying widely in their protections and in what information is covered, these laws require notice before data is collected and the ability to opt-out of the use and disclosure of personal information. At the same time the laws reward companies with less-burdensome reporting when the data is encrypted.

For biometric data, 16 states have included biometric-privacy language in their general data-privacy laws. This specific language includes:

STATUTORY LANGUAGE	NUMBER OF STATES
Medical history	12
Fingerprints	7
Biometric data	7
Retina or iris	6
DNA or genetic data	3
Human body characteristics	2
Voiceprint	2

More recently, states have sought to enhance protections on biometric data by proposing specific biometric information privacy laws. To date, at least seven states have considered related legislation and three have passed laws.

The most comprehensive of these new bioprivacy laws is the Illinois Biometric Privacy Act (BIPA), passed in 2008. To protect biometric-facilitated transactions, BIPA requires companies to:

- Make data-retention policies publicly available
- Give notice and receive consent before obtaining biometric identifiers and biometric information
- Refrain from selling biometric information to third parties
- Refrain from disseminating biometric information without prior written consent, absent certain exceptions
- Handle biometric information with reasonable care

Following the Illinois pattern, Texas passed the Capture or Use of Biometric Identifiers (CUBI) law, which protects biometric identifiers including "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry." Under CUBI, a company may not capture biometric data for commercial purposes unless the individual is informed before the capture and provides consent.

After the capture, a company may not sell, lease, or disclose the data without consent.

More recently, Washington state enacted its Biometric Identifiers law in 2017. It is narrower than BIPA and acknowledges situations where consent is not required (including fraud prevention).

These three laws hint at an emerging trend to render biometric data subject to heightened collection, storage and transmission protection standards.

iStock

Making important design decisions involving bioprivacy

Many states will continue to add to the types of data requiring additional protection and privacy considerations. In developing autonomous and/or connected systems that collect biometric data, engineers should consider the following:

- **Encryption:** biometric data should be transmitted and stored in an encrypted state to minimize potential legal risk
- **Consent:** systems should provide an opportunity to obtain the consent of each individual that has data being collected, and the consent of any parent or guardian for minors
- **Notice:** individuals that are providing biometric data should have full knowledge of the uses that will occur
- **Transparency in data-retention policies:** the data-retention policy for each system should be inconspicuously available.

As states move to provide heightened protections and the impact is felt from related global privacy regulations—including the European Union's General Data Protection Regulation (GDPR)—it is critical to emphasize privacy by design and to incorporate protections specific to bioprivacy. Engineers and designers must take note of these trends to incorporate the proper protections mandated by law, thereby leaving a privacy-oriented 'fingerprint' on the design. ■

A self-described "recovering engineer" with 15 years of experience in automotive design and quality, Jennifer Dukarski is a Shareholder at Butzel Long, where she focuses her legal practice at the intersection of technology and communications, with an emphasis on emerging and disruptive issues that include cybersecurity and privacy, infotainment, vehicle safety and connected and autonomous vehicles.