Bloomberg Law

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, 16 PVLR 1357, 10/9/17. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Legislation

Current Autonomous Vehicle Technology Standards for Privacy and Security: What are They and What Do They Mean?

Autonomous Vehicles

Criticism directed at the U.S. government for allegedly ''failing'' to promulgate privacy and security standards for autonomous vehicle technologies makes for a great sound bite, but critics of recent guidance and proposed standards fail to understand the U.S. ''norm'' of regulators looking for procedural compliance and evidence that they took seriously consumer privacy and security, the authors write.

By Mark Mao, Molly DiRago, and Jonathan Yee

There has been a flurry of recent criticisms against Washington, for allegedly ''failing'' to promulgate privacy and security standards for autonomous vehicle technologies. Such criticism makes for a great sound bite, but it fails to understand privacy and security standards in the U.S. Instead, the current proposals suggest that the U.S. will continue to follow data privacy and security precedence set by the Federal Trade Commission (FTC) for the last twenty years.

Mark Mao is a partner at Troutman Sanders LLP in San Francisco and is a member of the cybersecurity, information governance, and privacy practices and the business litigation practice.

Molly DiRago is an associate at Troutman Sanders LLP in Chicago and is a member of the business litigation practice.

Jonathan Yee is an associate at Troutman Sanders LLP in Irvine, Calif. and is a member of the cybersecurity, information governance, and privacy practice group with an emphasis on financial services litigation.

'The American Standard' for Data Privacy and Security

The U.S. follows a ''sectorial model'' for privacy, according to Foundations of Information Privacy and Data Protection. Unless a sector is covered by a privacy statute, such as the Gramm-Leach-Bliley Act (GLBA) for certain financial institutions, no general ''informational privacy'' rights apply. Instead, the privacy ''norms'' have thus far been formally and informally defined by regulators. The FTC is the most active and prominent amongst the regulators, typically policing all industries and practices where it is not preempted, to prohibit ''unfair and deceptive practices'' under Section 5 of the FTC Act.

''Privacy advocates'' often critique new laws and regulations for ''not doing enough,'' while ignoring that new law continues to follow the ''American norms'' of the last twenty years. Indeed, almost all law across all industries in the U.S. follow some form of the principles promulgated by the FTC over the last two decades:

a) Companies generally need to disclose their privacy practices to consumers, with regard to the collection, use, and dissemination of data. Thereafter, companies should follow what was promised in the disclosures.

b) Companies should make reasonable efforts to secure consumer information. At a minimum, such efforts

COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1538-3423

should include a written security plan, which evidences cybersecurity and due diligence. Due diligence is typically demonstrated by regular procedural testing against security standards accepted in the industry and is evidenced by documentation.

c) ''Sensitive personal information'' may require an express opt-in from the consumer as opposed to an opt-out. The FTC has pushed for geolocation data as sensitive information.

d) Anonymized information is not personal information. Information is anonymized when it cannot be reasonably linked to the individual from whom the information was originally collected.

In short, both data privacy and security are primarily procedural requirements in the U.S. Those who criticize the U.S. for ''lacking concern'' for privacy often confuse legal models focused on procedural safeguards with those focused on stated ''fundamental rights.'' Indeed, U.S. regulators consistently cite to standards embraced by the National Institute of Science and Technology (NIST), which are actually quite flexible and process-focused. The recent Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices guidance issued by the Food and Drug Administration, for example, are again heavily process-focused.

As it will be demonstrated below, these principles apply to the laws and regulations being proposed for the autonomous vehicle industry, including under the Trump Administration. Future legislation and regulations are likely to be commensurate with these principles.

The Current State of Federal Legislation and Regulations

There is currently no comprehensive federal privacy laws or regulations specific to autonomous vehicle technologies. However, regulatory guidance issued thus far and current Congressional bills suggest that the FTC's principles referenced above will likely continue to be the standard.

There are two noteworthy regulatory publications and one congressional bill that are indicative of the privacy laws and regulations likely to be in place in the future:

H.R. 3388, the 'Self Drive Act' In September 2017, the House of Representatives passed H.R. 3388, entitled the ''Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act,'' or the ''SELF DRIVE Act.''

By its current terms, the SELF DRIVE Act bill:

- Preempts new and existing state standards for the ''design, construction, or performance of highly automated vehicles, automated driving systems, or components of automated driving systems'' unless the standards are ''identical'' to what is promulgated under the SELF DRIVE Act. However, laws and regulations on vehicle registration and licensing as well as regulations on ''safety and emissions inspections, congestion management of vehicles on the street within a State or political subdivision of a State, or traffic'' shall remain within the province of the states unless such laws or regulations constitute an ''unreasonable restriction on the design, construction, or performance of highly automated vehicles, automated driving systems, or components of automated driving systems.''
- Provides that a manufacturer may not offer for sale or introduce into commerce any highly automated vehicle, vehicle that forms partial driving automation, or automated driving system unless such manufacturer has developed a cybersecurity plan that includes: (a) a written security policy that includes preventive measures, testing and monitoring, and updates, (b) limiting access to automated systems, and (c) employee training.
- States that a manufacturer may not offer for sale or introduce into commerce any highly automated vehicle, vehicle that forms partial driving automation, or automated driving system unless such manufacturer has developed a written privacy plan that describes: (1) how information of owners and occupants are collected, used, shared, and stored, (2) the choices available for owner and occupant privacy, (3) the manufacturer's practices with respect to data minimization, de-identification, and data retention, and (4) the privacy obligations of those who receive data from the manufacturer. Interestingly, the bill takes the position that ''information about vehicle owners or occupants [that] is altered or combined so that the information can no longer reasonably be linked'' to the vehicle, component, software, owner, or occupants, need not be included in the privacy policy. Violations of this provision shall be enforced by the Federal Trade Commission under Title 5 of the FTC Act.

NPRM Regarding Federal Motor Vehicle Safety Standard; V2V Communications (82 Fed. Reg. 3,854) Although not a cybersecurity document, the National Highway Traffic Safety Administration (NHTSA) and the Department of Transportation's (DOT's) NPRM for autonomous and connected cars ''proposes to establish a new Federal Motor Vehicle Safety Standard (FMVSS)'' to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions. The V2V communications focus heavily on the use of ''dedicated short-range radio communications (DSRC)'' devices to transmit ''Basic Safety Messages (BSM) about a vehicle's speed, heading, brake status, and other vehicle information to surrounding vehicles, and receiving the same information from them.'' The NHTSA claims that without such a protocol, the auto industry itself will be unable to move forward together meaningfully.

Consumer privacy and cybersecurity are at the heart-and-center of the proposals:

- The NHTSA ''proposes to exclude from V2V transmitting information that directly identifies a specific vehicle or individual regularly associated with a vehicle, such as owner's or driver's name, address, or vehicle identification numbers, as well as data 'reasonably linkable' to an individual,'' citing to the FTC.
- The ''NHTSA proposes V2V devices sign and verify their basic safety messages using a Public Key Infrastructure (PKI) digital signature algorithm . . . for BSM transmission and the signing of BSMs.''
- The ''NHTSA proposes to mandate requirements that would establish procedures for communicating with a Security Credential Management System to report misbehavior; and learn of misbehavior by other participants.''
- ''V2V systems would be required to be designed from the outset to minimize risks to consumer privacy.''

 COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

In addition to the peer-to-peer BSM communications, the NHTSA is requesting comments for two competing innovative proposals for V2V device credentialing, both of which would complement the use of PKI. The first approach is the ''Federated Security Credential Management (SCMS)'' model, which envisions a system ''established, funded, and governed primarily by one or more private entities—possibly a consortium of automobile and V2V device manufacturers.''

The NHTSA also is considering a ''Vehicle Based Security System (VBSS)'' as an alternative to SCMS, which has a single security certification root. The major difference is in the ''generation of short-term certificates.'' 82 Fed. Reg. 3,854 states: ''The SCMS approach relies on individual vehicles to periodically request pseudonym certificates from infrastructure-based entities (most notably a Pseudonym Certificate Authority, or PCA) which in turn generates and signs short-term certificates. Vehicles then download batches of certificates which are used to digitally sign BSM messages. In contrast, the VBSS concept calls for delegating this authority to individual vehicles, and as a result the communications with the infrastructure are reduced.''

The DOT's 'Automated Driving Systems: A Vision for Safety 2.0' In September 2017, DOT issued its voluntary guidance, Automated Driving Systems (ADS): A Vision for Safety 2.0, which is intended to update and replace the Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety, previously issued by the DOT in September 2016 under the Obama Administration.

The September 2017 guidance suggests ''12 priority safety design elements'' for Automated Driving Systems (ADSs), which are intended to help manufacturers ''be creative and innovative when developing the best method for its system to appropriately mitigate the safety risks associated with their approach.'' By its terms, the guidance states it applies to vehicles under the DOT's jurisdiction, including heavy-duty commercial vehicles. However, it focuses on vehicles with Automation Levels Three through Five, as defined by SAE.

Amongst the 12 priority design elements is the requirement that businesses conduct systematic and thorough planning and testing for cybersecurity, by using practices such as those promulgated by the NIST.

The Current State of State Legislation, Regulations, and Litigation

Adherence to general FTC guidance, supplemented with documented efforts to follow current federal guidance, will likely result in data practices that will be compliant with what is to follow shortly in the states as well. Not all states have regulations or guidance pertaining to autonomous vehicle technologies. Those that do—such as California—have proposed provisions like their counterpart federal guidance that generally refer to principles similar to those promulgated by the FTC. Notably, under the California proposal, anonymization is a defense to failure to disclose how data is used only if the data ''is not necessary for the safe operation of the vehicle.''

Other states follow the same model, and will likely continue following the same principles absent new precedence from the DOT. Notably, cyber-vulnerabilities of autonomous vehicle technologies have been the subject of contentious civil litigation, even where no accidents have actually occurred as a result of the alleged vulnerabilities. There are considerable differences amongst the circuits and state courts, however. Some product liability complaints based on cyber-vulnerabilities have survived pleading challenges, notwithstanding the fact that plaintiffs cannot allege actual out-of-pocket damages resulting from the vulnerability. In those cases, plaintiffs have been relying primarily on the theory that the vulnerability diminishes the value of the vehicles they purchased. Regardless, such litigation suggests that states will retain a strong voice in autonomous vehicle technology in areas relating to how data may affect vehicle safety, which are traditionally within the jurisdiction of the states.

Practical Considerations

In our experience, regulators and authorities are typically looking for procedural compliance. This means that they want to see documentation showing that the organization took consumer privacy and cybersecurity seriously. Most organizations—across all sorts of verticals—will be able to get by simply by checking and testing their designs and systems against industry guidance such as those promulgated by the NIST. Many critics of recent autonomous vehicle technology guidance and proposed standards have failed to understand this U.S. ''norm.''

However, where an organization becomes involved in a catastrophic or highly publicized data incident, regulators may judge the incident by the outcome, as opposed to the documentation showing due diligence. This is the exception, rather than the norm, however.

By Mark Mao, Molly DiRago, and Jonathan Yee

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com