PROGRAM MATERIALS
Program #3018
January 23, 2020

Self-Driving Gold Mines? Monetizing Big Data from Autonomous Vehicles and the Impact of Regulation

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

SELF-DRIVING GOLD MINES?

MONETIZING BIG DATA FROM AUTONOMOUS VEHICLES AND THE IMPACT OF REGULATION

January 23, 2020

orrick

Introductions

David Curtis
Associate
Cyber, Privacy & Data Innovation
dcurtis@orrick.com

Nick Farnsworth
Associate
Cyber, Privacy & Data Innovation
nfarnsworth@orrick.com

Agenda

- Autonomous Vehicles and Big Data
- Impact of Privacy and Data Security Regulation
- Contracting Considerations
- Key Takeaways

AUTONOMOUS VEHICLES AND BIG DATA

orrick

What is an Autonomous Vehicle ("AV")?

We use the term **Autonomous Vehicle** to refer to any Automated Vehicle capable of at least Conditional Automation.

Automated Vehicle: Any vehicle equipped with hardware and software that are collectively capable of performing part or all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic on a sustained basis, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints.

U.S. Department of Transportation, *Automated Vehicle 3.0: Preparing for the Future of Transportation (2018)*
(citing SAE International, *J3016* (revised 2018))

Practice Note: The media, industry, researchers and government use differing terms and definitions to describe vehicles with varying degrees of automation. As a result, you may see these terms defined differently in other settings.

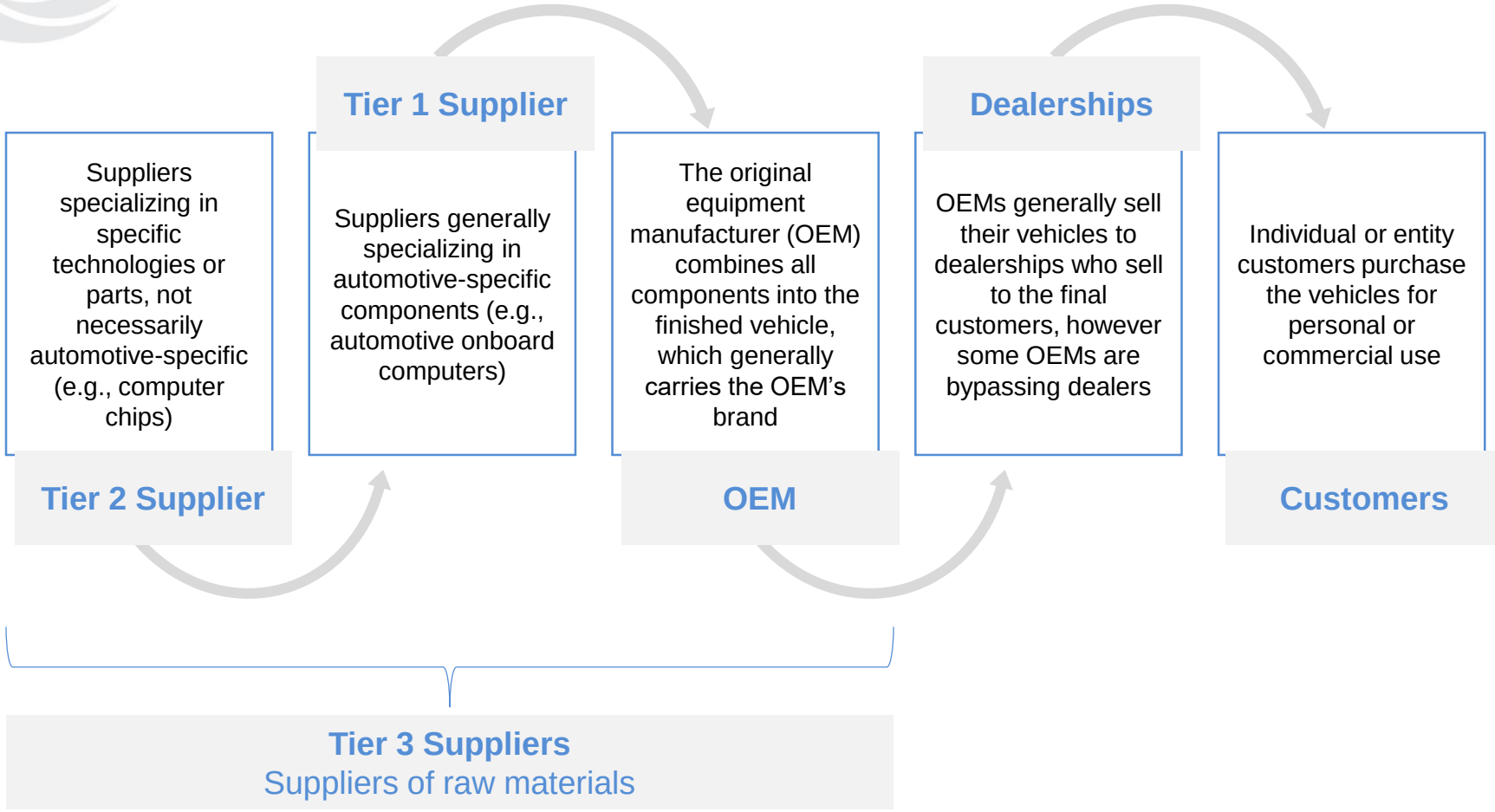
What is an Autonomous Vehicle ("AV")?

Levels of Automation: Like most of the AV industry, the U.S. DoT has adopted the six levels of vehicle automation defined in SAE International J3016:

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
No Automation	**Driver Assistance**	**Partial Automation**	**Conditional Automation**	**High Automation**	**Full Automation**
Driver performs all driving tasks; may benefit from active safety systems, such as alerts or intervention systems	Some automated driver assist features (steering OR acceleration/ deceleration), but driver performs remaining tasks	Automated steering AND acceleration/ deceleration features but driver must remain engaged	Mostly automated but driver must be ready to take control upon request or system failure	Fully automated under certain conditions; driver may have option to take control but not required	Fully automated under all conditions; driver may have option to take control but not required

U.S. Department of Transportation, *Automated Vehicle 3.0 (2018)*
(citing SAE International, *J3016* (revised 2018))

Autonomous Vehicle Supply Chain



Practice Note: Autonomous Vehicles may disrupt the traditional automotive supply chain. For example, OEMs may in the future choose to maintain ownership of AVs and generate revenue by charging customers for transportation, rather than selling all AVs to third-party owners.

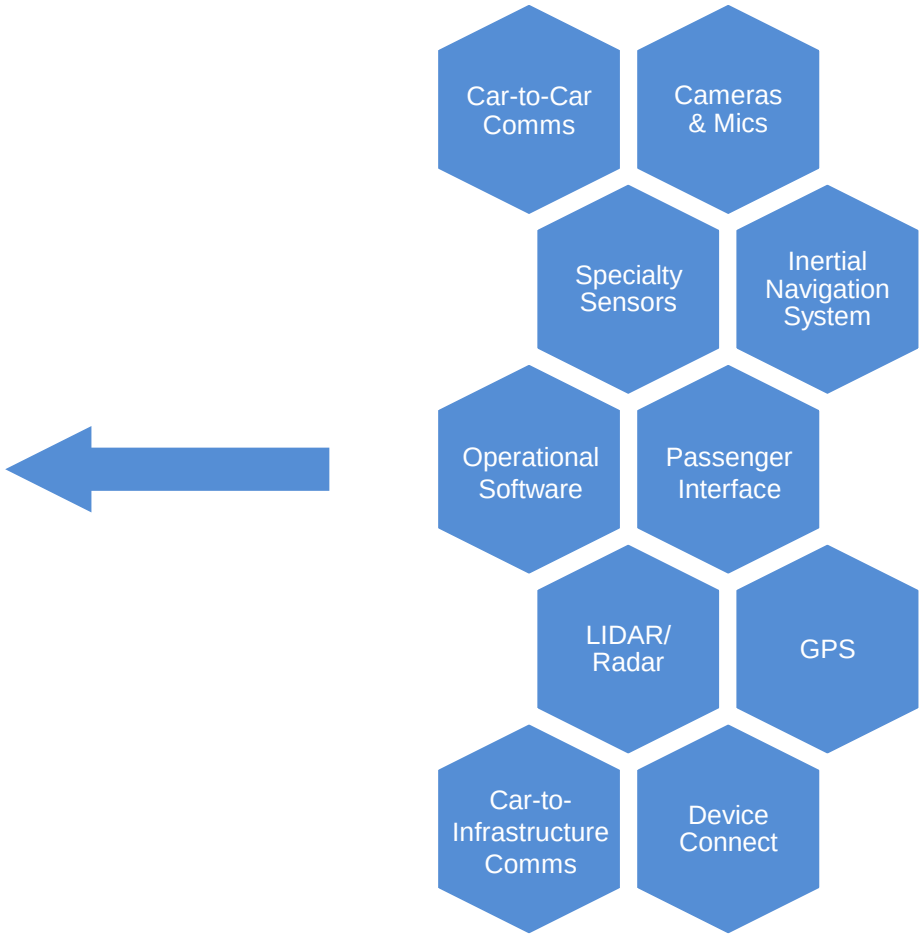
Autonomous Vehicle Technologies

Autonomous Vehicles rely on a combination of technologically advanced hardware and software to interpret its environment and drive safely.

Example Automated Features

- Autopilot
- Adaptive Cruise Control
- Adaptive Lighting
- Automated Parking
- Automatic Emergency Braking
- Automatic Pedestrian Braking
- Backup Camera
- Forward Collision Warning
- Highway Pilot
- Parking Sensors
- Rear Automatic Braking
- Rear Cross Traffic Alert
- Lane Centering Assist
- Lane Departure Warning
- Lane Keeping Assist
- Traffic Jam Assist

Automation: Combination of automated features to remove driver responsibility (wholly or partly)



Autonomous Vehicle Technologies

Global Positioning System (GPS)

System using satellites to triangulate a vehicle's precise geographic location

Lidar/Radar Sensors

Sensors using light (Lidar) or radio waves (Radar) to determine the distance between the vehicle and obstacles

Cameras & Mics

Devices used to capture actual images and audio of the vehicle's environment or cabin

Car-to-Car Comms

System used to allow vehicles to communicate with one another regarding the environment

Inertial Navigation System (INS)

System using internal accelerometers and gyroscopes to track a vehicle's position, orientation and speed

Specialty Sensors

Sensors using special technology (e.g., infrared) to detect specific objects in specific conditions (e.g., low light, close distance)

Device Connect

System used to connect third-party devices to the vehicle (such as mobile phones)

Car-to-Infrastructure Comms

System used to allow vehicles to communicate with infrastructure regarding the environment

Passenger Interface

Systems used to interface and communicate vehicle and trip-related information to the passenger (such as the vehicle's multimedia system)

Operational Software

Software used to interpret and operationalize all of the data collected from the vehicle's technologies for purposes of driving the vehicle and facilitating the desired trip

Autonomous Vehicle Data Collection

Essential Data

Data needed for an Autonomous Vehicle to operate safely and effectively:

- Vehicle statistics (e.g., speed, vehicle condition, fuel level)
- Weather, road and traffic conditions
- Vehicle proximity to other objects
- Advanced imagery used to track and predict object movement

Non-Essential Data

Data not needed for an AV to operate safely and effectively, or essential data used for non-essential purposes:

- Non-essential personal identification
- Non-essential passenger behavior and preferences
- Non-essential environmental analytics

Practice Note: The success of AVs will largely be determined by their ability to collect, process and execute upon an unprecedented volume of data. Experts are predicting this volume of data may surpass most processing activities carried out today, including a 2016 report by Intel estimating that AVs will generate approximately 4 terabytes of data per day. In addition, experts are predicting the overall revenue from car data monetization could be substantial.

Autonomous Vehicle Data Use Cases

Companies are developing unique ways of using combined sets of essential and non-essential data to differentiate themselves in the AV market, as well as to create additional cash flows relating to the sale and operation of AVs.

Data may be used for:

- Improving efficiency and performance of AVs
- Creating personalized passenger AV experiences
- Displaying personalized advertisements through the AV's entertainment system or on the surrounding environment using augmented reality
- Selling data relating to passengers (such as, travel preferences, destinations, interests) to data aggregators to improve consumer profiles for cross-sector advertising
- Using data relating to bystanders observed by AVs

IMPACT OF PRIVACY REGULATION

orrick

Impact of Privacy and Cybersecurity Regulation

Existing and anticipated privacy regulation has the potential to negatively impact the value and permissible use of data produced by Autonomous Vehicles, as well as the potential liability for AV manufacturers and operators:

- Regulation of children's data imposes exacting restrictions on the knowing collection, use and disclosure of children's personal information.
- Regulation of personal data sales may limit the ability to monetize AV data.
- Biometric laws limit the ability of Autonomous Vehicles to rely on biometric identifiers and increases the risk relating to its use.
- Restrictions on unfair and deceptive trade practices.
- Comprehensive laws granting consumers rights over data can impede the collection of non-essential data or non-essential use of essential data.

Inconsistent privacy requirements across federal, state and local law increase costs and make compliance a moving target.

Regulation of Children's Data

Throughout the world, businesses are often held to a higher standard in relation to children's privacy and lawmakers are starting to expand the applicability of children's privacy laws to new technologies.

Children's Online Privacy Protection Act (COPPA)

In the U.S., COPPA prohibits the collection of personal information from children under the age of 13 without the parents' verifiable consent by operators of online services knowingly collecting personal information from or directing services to children under the age of 13.

California Consumer Privacy Act (CCPA)

The CCPA prohibits a business from selling a California resident's personal information where the business has actual knowledge that the California resident is less than 16 years of age, unless proper affirmative authorization, either from the child or her parent depending on age, is obtained.

Regulation of the Sale of Data

Privacy laws are beginning to grant consumers rights to opt out of controversial uses of their personal information. In the United States, there has been a recent focus on the "sale" of personal information:

California Consumer Privacy Act (CCPA)

Broad Definition of "Sale": Making available or transferring personal information to a third party for monetary or other valuable consideration.

Broad Applicability: Applies to the "sale" of personal information collected about California residents both online and offline, and the business is required to clearly provide a "Do Not Sell My Personal Information" link on digital properties.

Nevada Privacy Law (SB 220)

Narrow Definition of "Sale": Exchange of covered information for monetary consideration by a website operator to a person for the person to license or sell to third parties.

Narrow Applicability: Applies only to certain "covered information" collected through a website or online service, and the business need only provide a designated address for submitting the request.

A right to opt-out of the "sale" of personal information could impede a company's ability to monetize data from Autonomous Vehicles.

Biometric Laws

Many advanced technologies use biometrics to verify user identities without inconveniencing the user in the process. AVs are likely to rely in part on biometrics to verify the identities of AV owners and passengers.

- Existing state privacy laws, like the Illinois Biometric Information Privacy Act, impose strict obligations on a company's collection of and care for biometric information.
- Biometric information technology is often produced by third-party specialists and integrated into larger technology platforms, meaning AV operators may have little control and oversight over these features.
- Biometric information technology can be susceptible to implicit bias that could result in unintentional disparate treatment of certain populations.
- Legislators are beginning to take an even harder look at the use of biometric information, particularly in relation to surveillance by the government which could be a large customer of AV data.

These laws introduce increased costs for compliance, restrict the ability of AV OEMs and Tier 1 Suppliers to process biometric information and raise the risk profile for impacted companies.

Illinois Biometric Information Privacy Act (BIPA)

Applies to private entities collecting or possessing biometric identifiers or biometric information. Requiring them to:

- To disclose a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.
- Prior to obtaining the biometric identifier or information:
  - To inform the data subject that a biometric identifier/information is being collected/stored;
  - To inform the data subject of the specific purpose and length of term for which the biometric identifier/information is being collected, stored and used;
  - To receive a written release executed by the data subject.

Practice Note: Class actions have been popular under BIPA's private right of action available to persons "aggrieved" by statutory violations of BIPA's privacy and security obligations, with "liquidated damages" of $1,000 per negligent violation and $5,000 per intentional or reckless violation.

Unfair and Deceptive Trade Practices

- The FTC Act (§5) and similar state laws regulate **unfair** and **deceptive** trade practices.
  - **Unfair**: conduct that causes or is likely to cause substantial injury to consumers and is not reasonably outweighed by countervailing benefits.
    - E.g., unreasonably weak data security practices
  - **Deceptive**: a material misrepresentation or omission that is likely to mislead a consumer acting reasonably under the circumstances.
    - E.g., material failure to disclose data sharing practices in consumer-facing privacy policy
- Risk Exposure
  - Cease and desist order
  - Injunctive relief
  - Restitution

Comprehensive Privacy Laws

Comprehensive privacy legislation has been gaining momentum in recent years, with federal and state governments passing laws across the globe.

General Data Protection Regulation

The European Union's comprehensive privacy regulation enforceable as law in all EU Member States as of May 2018

California Consumer Privacy Act

The state of California's comprehensive privacy law that took effect January 2020

Lei Geral de Proteção de Dados Pessaoais

Brazil's comprehensive privacy law inspired by the EU's GDPR, taking effect August 2020

The U.S. Congress continues to consider comprehensive federal privacy legislation. In addition, many states considered CCPA-like bills in 2019 and may propose similar bills in 2020.

EU General Data Protection Regulation

Generally applies to (i) processing of personal data relating to a business's establishment in the EU or (ii) processing of personal data of data subjects located in the EU relating to a business's offering of goods/services to or monitoring the behavior of data subjects in the EU.

DISCLOSE:

- categories of PD it processes, how PD is retained, shared and transferred internationally;
- categories of sources of the PD;
- purposes and legal basis for processing PD; and
- description of the consumers' rights and the designated methods for submitting requests.

PROVIDE ACCESS:

- to PD being processed by the business and a ***portable*** copy of the PD provided to the business by the data subject.

RECTIFY:

- inaccurate PD upon request.

ERASE:

- PD concerning the data subject, subject to exceptions.

PERMIT RESTRICTION:

- to processing of PD in certain circumstances.

PERMIT OBJECTION:

- to processing of PD in certain circumstances, including to direct marketing purposes.

PROHIBITS PROCESSING:

- of special categories of PD (e.g., biometric info) unless an exception applies.

PROHIBITS TRANSFERS:

- internationally to other countries without adequate safeguards in place.

CONTRACTS*:*

- with third parties processing PD on a business's behalf must be governed by a contract restricting processing only on the business's instruction.

The California Consumer Privacy Act of 2018

Generally applies to for-profit entities (i) doing business in California, (ii) collecting, receiving or accessing CA resident's personal information, (iii) deciding why and how personal information is used or processed and (iv) satisfying a quantitative threshold (e.g., $25M gross revenue).

DISCLOSE:

- categories of PI it collects, sells and otherwise discloses for a business purpose;
- categories of sources of the PI;
- business or commercial purposes for collecting or selling the PI; and
- description of the consumers' rights and the designated methods for submitting requests.

PROVIDE ACCESS:

- to the PI collected over the past 12 months in a portable format, in response to a "verifiable consumer request".

DELETE:

- PI upon a "verifiable consumer request" (and direct "service providers" to delete), subject to exceptions

PERMIT OPT-OUT:

- of data "sales" to third parties (including via "Do Not Sell My Personal Information" link), subject to exceptions

OBTAIN OPT-IN CONSENT:

- for children under 16, for "sales" of PI to a third party ("actual knowledge" and willfully disregard" standard)

TRAIN EMPLOYEES:

- about the business' privacy practices, compliance and how to direct consumers to exercise their rights

NOT DISCRIMINATE:

- Against consumers who exercise their rights under the CCPA, but some financial incentives permissible ("Pay-for-Privacy")

CONTRACT *effectively*:

- relative to "service providers" to establish scope of permissible data uses and mechanism for complying with consumer access/deletion requests

IMPACT OF CYBERSECURITY REGULATION

orrick

Cybersecurity Threats

Autonomous Vehicles will rely on increasingly complex connected networks to share and analyze data to operate efficiently, effectively and profitably. This complexity leads to cybersecurity risk for AV operators, passengers and the general public:

Personal Data Breach

Unauthorized access or acquisition of certain personal sensitive personal data (e.g., biometric data) requiring notification

Malware/ Ransomware

Software designed to disrupt or damage an AV, which could result in an inability to drive creating dangerous situations

Vehicle Takeover

Unauthorized control of the AV by a malicious actor intending to cause personal inconvenience, property damage or physical harm

Real-Time Passenger Tracking

Unauthorized access to passenger travel logs or location could pose a threat to vulnerable populations (e.g., domestic violence)

Connected Environment Attack

Attackers using less secure connected devices to bypass security and gain unauthorized access to an AVs system or data

Network Takeover

Unauthorized control of a network of AVs or infrastructure by a malicious actor intending to cause widespread harm and terror

Cybersecurity Regulation

The AV industry is likely to be subject to new cybersecurity regulation, including:

Breach Notification Laws

Companies may be subject to notice obligations or private rights of action in the event of unauthorized access or acquisition to certain covered information.

Internet of Things Cybersecurity Laws

California's new IoT law (SB 327) became the first U.S. cybersecurity law specifically governing connected devices, requiring manufacturers to equip connected devices with "reasonable" security.

Industry Standards

Several regulators and industry groups have been pushing to develop industry standards for automotive cybersecurity, including the National Highway Traffic Safety Administration.

Critical Infrastructure

Vehicle manufacturing and transportation systems are already considered critical infrastructure sectors subject to regulation by the U.S. Department of Homeland Security.

CONTRACTING CONSIDERATIONS

orrick

Who "Owns" AV Data?

Competing Ownership Interests

If Autonomous Vehicle data is as valuable as experts are predicting, many AV market players will want to stake a claim in data ownership:

- **AV operators**, such as ride share companies, may wish to own non-essential data relating to their customers or the operation of the AVs;
- **OEMs**, as the compilers and sellers of the finished AV product, may wish to own data relating to the individuals that purchase their AVs and other individuals that interact with their AVs (either as passengers or bystanders);
- **Suppliers**, as the providers of individual AV components and technologies, may seek to own the data collected by those particular components and technologies;
- **End customers** may be legally entitled to certain rights with respect to the data AVs collect about them, including rights to restrict what AV market players collect and how they use it.

What Does It Mean to "Own" Data?

- **Intellectual Property**
  - **Copyright:** The data must have a minimal amount of creative expression (originality) and must be fixed in a tangible medium.
  - **Patent:** The patentable invention must be novel, non-obvious, and useful.
  - **Trade Secret:** The data (1) must be, or potentially be, economically valuable because it is not known or able to be discerned by others who otherwise could benefit economically from using or disclosing it and (2) it is protected by reasonable efforts to maintain its secrecy.
- **Intangible Property Rights**
  - Property that has value but cannot be seen or touched.
  - Case law treats data like any other property by according it certain common law protections, e.g., trespass to chattels.
- **Contract Rights**
  - **"Confidential Information"** - restrict use of data one party shares with another
  - **Licenses** - can be express or implied

Data Licensing Agreements 101

- **What is a Data Licensing Agreement?**
  - A contract where an owner of data (**"licensor"**) grants to another party (**"licensee"**) certain rights to use that data.
  - A Data Licensing Agreement set forth the limitations on the licensee's use of the data, as well as the allocation between the parties of the obligations, risks, and royalties regarding the data.
- **Why are Data Licensing Agreements important in the AV context?**
  - Opportunity to address the various competing and overlapping interests in AV data across the AV development and supply chain.
  - Formalize the licensor's ownership interests, and establish the licensee's data use rights.
- **When should parties address data ownership and data licensing issues?**
  - Early on in the AV development process.

Data Licensing – Key Considerations

What data is being licensed? By whom? To whom?

What is the business objective?

Type of data and deployment model

Ownership in data and derivatives

Scope of license based on business needs

How is data intended to be used and how might it otherwise be used?

What are the regulatory and contractual compliance requirements?

What measures are required to decrease risk and increase compliance?

Example: Representations and Warranties

- **IP** - Do not assume Intellectual Property reps and warranties cover data. Revise to address material data (and algorithms) as appropriate.
- **Security** - Consider including **all** intangible data, not just personal data, in data privacy and cybersecurity warranties.
- **Artificial Intelligence** - Consider warranties that data used to train AI models is correct, an appropriate set of data and without bias.
- **Sufficiency of Assets** - Review sufficiency of assets warranties to ensure it includes rights in data.
- **Liens** - Review warranties on liens and encumbrances for any potential issues based on data usage.

Example: Contracting to Avoid CCPA "Sales"

- Proper contract terms can relieve a CCPA-covered business from its obligation to provide California residents the right to opt out of the sale of personal information.
- NOT a "sale" where personal information is disclosed to a:

Service Provider

- A for-profit entity that processes PI **on behalf of a business** and for a "business purpose"
- Must have a **written contract** that prohibits **retaining, using or disclosing** the PI for any purpose (including any commercial purpose) other than:
  - performing the services specified in the contract for the business; OR
  - **as otherwise permitted by the CCPA**

OR

"Certified" Partner

- A **person** that receives PI for a **"business purpose"** pursuant to a **written contract** that:
  - prohibits the person from **selling the PI**;
  - prohibits retaining, using or disclosing the PI for any purpose (including any commercial purpose) other than performing the services specified in the contract;
  - prohibits retaining, using or disclosing the PI **outside of the direct business relationship** between the person and the business; AND
  - **includes a certification** that the person understands the above restrictions and will comply with them

Example: “Reasonable” Security

- To mitigate cybersecurity risk, AV data licensors should consider seeking “reasonable” data security commitments from licensees and vendors:
  - Security measures in accordance with industry standards (NIST, ISO, etc.)
  - Written information security program
  - Ongoing risk assessment and management
    - Table-top exercises
    - Penetration tests
  - Employee training
  - Vendor management (require similar downstream contracting)
  - Incident response plan
  - Audit rights
    - Independent third-party audits
    - Reserve right for licensor to conduct audits

Other Contracting Considerations

- **Derivative Works** – Should the licensee have the right to anonymize/aggregate data for its own use? Can the data be used for machine learning purposes?
- **Data rights v. confidentiality terms** – Do restrictions on use of confidential information have an unexpected impact on the licensee's rights to use data?
- **Indemnification** – Consider carving regulatory fines/penalties out of limitations on liability and exclusions for consequential damages.
- **Cybersecurity Insurance** – Consider adding cyber insurance requirements to mitigate risk.

KEY TAKEAWAYS

orrick

Key Takeaways

Because of the potential value generation from Autonomous Vehicles and their ability to generate big data, companies should consider:

- Determining ownership of data collected and generated by AVs and AV components.
- Understanding the impact comprehensive and sector-specific privacy laws may have on the ability to use AV data and the value it may present.
- Structuring comprehensive privacy programs in a way that can help the company enable the use of AV data while respecting consumer privacy rights.
- Understanding the cybersecurity risks relating to AVs and AV data, and building flexible solutions for mitigating and responding to potential security incidents.
- Actively considering the value of data generated from the sale and operation of AVs and AV components.
- Contracting to assert ownership rights and mitigate risks

QUESTIONS?

orrick

David Curtis

Associate

Seattle, Boston

T +1 206 839 4338

E dcurtis@orrick.com

Honors

- Harvard Law School, 2015, Dean's Award for Community Leadership

Education

- J.D. Harvard Law School, 2015
- B.A., Yale University, 2011, cum laude

David Curtis is a member of Orrick's internationally-recognized Cyber, Privacy & Data Innovation practice.

David's practice focuses on data privacy, cybersecurity, digital advertising, Internet law and consumer protection. David advises clients on data collection, storage, use, licensing and transfer issues. He also provides guidance on issues relating to the California Consumer Privacy Act of 2018 (CCPA), the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and other state and federal laws and self-regulatory frameworks. In addition, David has experience evaluating the applicability of European data protection requirements to U.S. companies.

Before joining Orrick, David was an associate at Ropes & Gray LLP and an adjunct professor at Harvard Law School, where he taught legal research, writing and analysis. David clerked for Justice Barbara Lenk of the Supreme Judicial Court of Massachusetts.

To make the California Consumer Privacy Act ("CCPA") more accessible, David was a member of the team that developed Orrick's CCPA Readiness Assessment Tool. The tool provides companies an opportunity to test their preparedness for compliance with the CCPA as a first step to constructing their strategic compliance roadmap.

Nicholas Farnsworth

Associate

Boston

T +1 617 880 1855

E nfarnsworth@orrick.com

Education

- Georgetown University Law Center, J.D., 2017, Magna Cum Laude; Order of the Coif; Executive Editor, The Georgetown Law Journal
- Harvard College, A.B., Economics, 2012

Privacy and cybersecurity underpins the innovative strategies of businesses across all sectors and introduces both legal and operational concerns. As a member of Orrick's internationally recognized Cyber, Privacy & Data Innovation team, Nick Farnsworth advises clients on a broad range of privacy and cybersecurity matters, including compliance, risk management and incident response.

Nick's practice focuses on guiding clients through the existing patchwork of state, federal and international privacy and cybersecurity laws. His practice includes advising clients on Section 5 of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), the Telephone Consumer Protection Act (TCPA), CAN-SPAM, state breach notification laws and state privacy and cybersecurity laws, such as the California Consumer Privacy Act. Nick also advises clients on the impact of international laws from a U.S. perspective, including the European Union General Data Protection Regulation (GDPR).

Nick assists clients from a broad range of industries and sectors in assessing their current privacy and cybersecurity practices. He regularly assists clients in developing global privacy and cybersecurity programs to practically implement the principles and obligations underlying various legal regimes, as well as assessing proposed marketing/advertising, transactional and business strategies from a privacy and cybersecurity perspective. Nick also advises clients on the assessment of suspected incidents/breaches and any associated notification obligations, as well as the privacy and cybersecurity risks associated with proposed transactions and ventures.

In addition, Nick has an active pro bono practice, which has included representing clients in immigration and innocence matters and assisting small businesses with their legal needs.

To make the California Consumer Privacy Act (“CCPA”) more accessible, Nick was a member of the team that developed Orrick's CCPA Readiness Assessment Tool. The tool provides companies an opportunity to test their preparedness for compliance with the CCPA as a first step to constructing their strategic compliance roadmap.

Trust Anchor

An established point of trust in a cryptographic system from which a process of validation can begin

Blog: blogs.orrick.com/trustanchor
Twitter: @Trust_Anchor

Supplemental Articles by Orrick (full articles follow):

- FTC Staff Issues Comments Discussing Key Security and Privacy Issues Surrounding Connected and Automated Vehicles (Feb. 22, 2018)
- California Sets the Standard with a New IoT Law (Nov. 14, 2018)
- Nevada Passes Opt-Out Law, Effective October 2019 – Three Months Before the CCPA (June 10, 2019)
- Roller Coaster Start to the New Year for Biometrics: Rosenbach v. Six Flags and Emerging Biometric Laws (Feb. 14, 2019)
- The CCPA Is in Effect and It Is Not Too Late to Get Started in 2020 (Jan. 2, 2020)

Supplemental External Government Publications (Please click the link):

- The National Science & Technology Council and the U.S. Department of Transportation's *Ensuring American Leadership in Automated Vehicle Technologies Automated Vehicles 4.0* (January 2020): https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf
- The U.S. Department of Transportation's *Preparing for the Future of Transportation Automated Vehicles 3.0* (October 2018): https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf


orrick

orrick

Cyber, Privacy & Data Innovation Alert

February 22, 2018

FTC Staff Issues Comments Discussing Key Security and Privacy Issues Surrounding Connected and Automated Vehicles

by **Jennifer R. Martin** | **Diana Fassbender** | **Melanie D. Phillips**

Given the explosive growth in the connectivity of every day "things," several government agencies are focused on how best to support innovation and the benefits of an increasingly connected, data driven society, while weighing options for mitigating the cybersecurity and privacy risks relating to the Internet of Things.[1] The pace of development with respect to connected cars and autonomous vehicles has drawn particular attention.

Most recently, in January 2018, the Federal Trade Commission (FTC) issued a "*Staff Perspective*" on the Connected Cars Workshop hosted by the FTC and National Highway Traffic Safety Administration (NHTSA) last June 28, 2017. Workshop participants included representatives from across private industry, government agencies, consumer groups, and academia. While the FTC recognizes that autonomous vehicles have the "potential to revolutionize motor vehicle safety," the Staff Perspective summarizes the key takeaways from the one-day workshop specific to discussions around consumer privacy and cybersecurity concerns associated with connected vehicles.

1. *A Variety of Stakeholders in the Connected Car Ecosystem will Collect Data for Different Purposes*

The Staff Perspective recognizes that a range of organizations in the connected car environment will collect data from vehicles, including not only vehicle manufacturers, but insurers, app developers, and other entities that provide services such as entertainment content delivery, regulatory diagnostics, and features yet to be developed. Much of this data will be used for safe vehicle operation, such as vehicle-to-vehicle (V2V) speed and position data used to navigate traffic and avoid accidents. However, developers of infotainment systems, for example, may collect and use data to enable consumers to utilize functions such as navigation, music, phone contacts, and the Internet. Similarly, third-party providers may collect and transmit information about consumer driving habits for diagnostics and big data analytics, including, for example, to price insurance.

Workshop participants recognized that certain data uses are critical to autonomous vehicle use and safety, while other data collection is merely for consumer convenience. Other uses were perceived as harmful; for example, some participants expressed concern about insurance companies using driving data to raise rates or penalize safe drivers who opt out of data collection.

2. *The Sensitivity of Data Collected Will Vary*

The Staff Perspective also recognizes that the sensitivity of the collected data will vary across the privacy spectrum. Specifically, participants recognized degrees of privacy concerns ranging from those associated with less sensitive anonymized, aggregate data used for traffic management purposes, to information about specific vehicle performance and gas mileage, for example, to highly sensitive personal information showing driver location or biometric data used for authentication purposes.

3. *Data May be Used for Unexpected Purposes*

Because of the range and volume of data collected, the Staff Perspective further recognizes that consumers might be concerned about "secondary, unexpected" uses of the data, such as the sale of personal information to third parties who in turn use the information to target products to consumers. Accordingly, participants discussed transparency about data collection and use, and consumer consent and opt-out options.

With respect to these three key issues associated with the collection and use of a variety of types of data associated with connected vehicles, participants at the workshop underscored the importance of addressing privacy concerns to encourage consumer adoption of connected car technologies. Workshop participants discussed the need to consider different approaches to data collection and use depending on whether the particular data being collected is necessary for safety and autonomous vehicle operation or, conversely, whether it involves personal information collected for non-critical uses. Participants also noted the need for consumer input, education, and choice.

The Staff Perspective recognizes the important initiatives already underway in the industry, including the Consumer Privacy Principles of the Alliance of Automobile Manufacturers and Global Automakers and the collaboration between the National Automobile Dealers Association and the Future of Privacy Forum to produce consumer education about the information that may be collected, guidelines for collection and use, and consumer options for such collection and use.

4. *Cybersecurity Concerns*

Finally, the Staff Perspective also summarizes workshop discussions focused on the cybersecurity risks posed by connected and autonomous vehicles. Noting that hackers no longer need physical access to a vehicle to cause harm, participants recognized that malicious actors pose a myriad of potential threats. External actors can hack into a single vehicle for malicious purposes, attack a large number of connected cars simultaneously, or target our transportation systems to cause significant risks to public safety and welfare.

The Staff Perspective describes several cybersecurity best practices to address some of the security risks associated with connected vehicles, including (i) sharing threat intelligence and vulnerability information through industry groups; (ii) specific network design solutions such as, for example, segregating safety functions from non-critical safety functions; (iii) risk assessment and mitigation throughout the vehicle lifecycle (from design and development through end-of-life); and (iv) industry self-regulation and standard setting to establish baseline security measurements.

Lastly, the Staff Perspective notes a couple of pertinent developments since the workshop took place last June. In particular, the NHTSA and U.S. Department of Transportation released new federal guidance pertaining to automated vehicles, *Automated Driving Systems 2.0: A Vision for Safety*, on September 12, 2017. In addition, the U.S. House of Representatives passed the Safely Ensuring Lives Future Development and Research in Vehicle Development (SELF DRIVE) Act (H.B. 3388) (*https://energycommerce.house.gov/selfdrive/*). The *bill* would require autonomous vehicle manufacturers to develop written cybersecurity and privacy plans. The bill also would require the NHTSA to develop a rulemaking and safety priority plan for highly autonomous vehicle standards and require the FTC to conduct a study and submit a report to Congress on privacy issues relating to the highly autonomous vehicle ecosystem. Although not discussed in the Staff Perspective, we also note that the U.S. Senate introduced The American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) (S. 1885) in September 2017 that proposes a variety of legislative changes relating to the development of self-driving transportation.[2] However, the AV START bill hit a roadblock in the Senate in early February 2018: according to reports, at least three senators have placed holds on the bill due to concerns about safety and that the bill does not go far enough to regulate developers of autonomous

vehicles.[3] Consequently, issues surrounding autonomous and connected cars will likely be a continued point of discussion by Congress in the coming months.

Given the rapid pace of development in vehicle automation and connectivity, industry, government, consumer groups, and other stakeholders will undoubtedly continue to collaborate on best practices and examine policy to strike a balance between innovation and consumer protection.

_____

[1] Bryan Koenig, *FTC Chief Says Connected Cars Require 'Regulatory Humility'*, Law360 (June 28, 2017), https://www.law360.com/articles/939274/ftc-chief-says-connected-cars-require-regulatory-humility-.

[2] Office of U.S. Senator John Thune (September 28, 2017), *Thune Introduces Bipartisan Autonomous Vehicle Legislation [Press Release]*, retrieved from *https://www.thune.senate.gov/public/index.cfm/2017/9/thune-introduces-bipartisan-autonomous-vehicle-legislation*.

[3] John D. McKinnon, *Self-Driving Car Legislation Stalls in the Senate*, Wall Street Journal (February 12, 2018).

---

orrick

Cyber, Privacy & Data Innovation Alert

November 14, 2018

California Sets the Standard With a New IoT Law

by **Jennifer R, Martin** | **Kyle Kessler**

This past September Governor Brown signed into law Senate Bill 327, which is the first state law designed to regulate the security features of Internet of Things (IoT) devices. The bill sets minimum security requirements for connected device manufacturers, and provides for enforcement by the California Attorney General. The law will come into effect on January 1, 2020, provided that the state legislature passes Assembly Bill 1906, which is identical to Senate Bill 327.

Connected devices are already part of our everyday lives, and will increasingly include a large number of the consumer products we use daily, including automobiles, smart TVs, home monitoring and management systems, toys, wearable health-related monitors, and a range of appliances. Moreover, critical industries, including the transportation, manufacturing, agriculture, healthcare, and energy sectors, are increasingly relying on data from sensors and smart devices to increase efficiencies, reliability and accuracy in delivery of services and products. Our city landscapes are also changing with the integration of smart traffic lights, smart lighting, smart cameras, smart buildings, and smart security.

While this ubiquitous interconnectivity will bring substantial benefits in terms of increased analytic accuracy and diagnostics, productivity and efficiency in the provision of services, and advances in public health, hackers will also find ways to exploit vulnerabilities in IoT devices to steal data, cause outages, disrupt or modify system functions, and commit other malicious acts.

The new law is intended to address these threats by requiring manufacturers to build security into the design, manufacturing, and functioning of connected devices.

Who does the law apply to?

The law applies to manufacturers of “connected devices” sold or offered for sale in California, as well as component parts suppliers for such manufacturers. Manufacturers and third-party parts suppliers are required to ensure that “connected devices” incorporate “reasonable security features” designed to protect the device and the data collected, stored, or transmitted on the device, from unauthorized access, destruction, use, modification, or disclosure. The law specifically exempts from coverage developers of third-party software or applications that consumers themselves may add to their connected devices and businesses regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

What is a connected device?

Under the new law, a “connected device” is defined as “any device, or other physical object that is

- capable of connecting to the Internet, directly or indirectly, and
- assigned an Internet Protocol address or Bluetooth address.”

In other words, if a product or "thing" can communicate and interact over the Internet, and can therefore be remotely accessed, monitored and controlled, then it is a connected device. Because the law is intended to mitigate the risk of unauthorized access to those networked devices that are a part of the Internet of Things ecosystem, if a device is only accessible with a local connection (i.e. on the same Wi-Fi network, or using Bluetooth only, with no control from the Internet), it does not fall under the definition of a connected device.

What is technically required?

If you are a manufacturer of a connected device or one of its component parts, then the law requires you to

- Ensure the device is equipped with "reasonable security features"; and
- Complies with the specific authentication requirements that are described more fully below.

1. Reasonable Security Features

Although the IoT law does not define what "reasonable security features" means, it does recognize that the "reasonableness" of security safeguards are risk-based and highly dependent on the type of product, its intended use, and the technology on which it relies. Specifically, the law states that a connected device's security features must be:

- appropriate to the nature and function of the device;
- appropriate to the information it may collect, contain, or transmit; and
- designed to protect the device and any information contained in the device from unauthorized access, destruction, use, modification, or disclosure.

Although this requirement is consistent with the risk-based principles for assessing "reasonable security" in traditional cybersecurity contexts, it does not provide much practical guidance to manufacturers of connected devices. Notwithstanding this inherent ambiguity, lawmakers and regulators have started to promulgate guidance documents on best practices and standards, primarily on an industry-by-industry bases. For example, the Federal Trade Commission (FTC), which has broad authority over consumer product safety under section 5 of the FTC Act, issued the Internet of Things Privacy & Security in a Connected World guidance document in 2015. The FTC has also taken enforcement action against connected device manufacturers, thus developing a set of regulatory expectations for manufacturers with respect to cybersecurity. See, e.g., In the Matter of TrendNet Inc. (Jan. 2014); In the Matter of ASUSTeK Computer, Inc. (Feb. 2016). In the eHealth industry, the Federal Drug Administration (FDA) has promulgated several guidance documents relating to the development and manufacturing processes associated with the security of connected medical devices, as well as the continuing post-market expectations on manufacturers to secure devices throughout their lifespan. See Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (10/2014) and the Postmarket Management of Cybersecurity in Medical Devices.

Similarly, the FTC and the National Highway Traffic Safety Administration (NHTSA) held a workshop on security and safety of autonomous vehicles in June 2017, in part to discuss developing standards.

Finally, for those IoT manufacturers who sell to the federal government, in 2017 the Senate passed a bill entitled the Internet of Things Cybersecurity Improvement Act of 2017 (S. 1691), which would establish security requirements and a certification processes for manufacturers that supply connected devices as government contractors.

2. Authentication Features

The CA law also contains specific requirements on authentication features to address access to IoT devices. If a product or device is connected to the Internet such that it is assigned an IP or Bluetooth address for authentication purposes, then the law requires that the default password to access or use the device must be

unique (i.e. the same pre-programmed or hard-coded password may not be used across devices); or, functionally, the users are required to generate a unique password at the time of first use or access.

The law's focus on authentication likely stems, in part, from the Mirai botnet attacks that caused significant website outages in October 2016. In that attack, hackers exploited a hardcoded default password in the firmware of a particular component part used in home routers and video recorders (DVRs) to take control of millions of those devices to attack critical systems on which the world wide web depends.

Enforcement & General Regulatory Framework

The California State Attorney General, as well as local city, county and district attorneys, are charged with enforcing the new law. The law does not establish a private right of action for alleged violations. However, the law does not preclude potential civil claims or enforcement by federal regulators, including the FTC for "unfair" and "deceptive" practices.

What can manufacturers do now?

In short, what constitutes reasonable security features in connected devices will be highly dependent on the risks posed by the particular technology and product – for example, what is reasonable security for a refrigerator may be different from what is reasonable for an implanted heart defibrillator. Despite the lack of clear guidance on what "reasonable security" means, the following baseline features for IoT manufacturers to consider in setting up their product development programs can be gleaned from current regulatory guidance:

- Security by Default: Security features should be built into the product from design inception and considered throughout the product's lifespan.
- Secure Software Development Lifecycle (SSDL): Developers should be trained in and comply with established software development best practices (e.g., ISO/IEC 27034-1).
- Supply Chain Diligence: Manufacturers should conduct due diligence on their component parts manufacturers
- (hardware, firmware, and software) and impose contractual requirements to ensure they are also following security best practices.
- Integrity of the Development Process: Manufacturers should ensure employees are adequately trained on security; the development environment and Intellectual Property are properly protected; and standard quality assurance processes are followed.
- Ongoing Monitoring and Maintenance: Because security extends beyond the factory floor, programs should be developed for post-marketing patching, monitoring, vulnerability handling, and product end-of-life practices.

Moreover, in developing an IoT device, there may be a host of other privacy issues to consider with respect to the collection, processing, and transmission of data. This is especially important if your device will be collecting children's data.

Orrick is here to assist you design an IoT product development program that will meet the objectives of the California law, and prepare you for the increased focus by federal and state legislators and regulators on IoT safety and security concerns.

---

orrick

Cyber, Privacy & Data Innovation Alert

June 10, 2019

Nevada Passes Opt-Out Law, Effective October 2019 – Three Months Before the CCPA

by **Emily Tabatabai** | **Melanie D. Phillips** | **Kyle Kessler**

Following in California's footsteps, Nevada has passed a new privacy law providing consumers the right to opt out of the sale of their personal information. Senate Bill 220 (SB-220), signed into law by Governor Steve Sisolak on May 29, 2019, amends Nevada's existing online privacy statute, NRS 603A.340, to include a requirement that online operators provide consumers with a means to opt out of the sale of specific personal information collected by websites or online services. The act goes into effect on October 1, 2019 – three months ahead of the January 1, 2020 effective date of the California Consumer Privacy Act (CCPA) – which may force companies to fast track implementation efforts for opt-out requests in particular.

Statutory Coverage and Key Definitions

Though similar in concept to the CCPA's right to opt out, the scope and coverage of Nevada's law is far narrower than the California law and does not provide any other consumer rights to access or delete personal information. In contrast to the CCPA's coverage of both online and offline businesses, the Nevada law applies only to online "**operators**" who own or operate a website or online service for commercial purposes and who collect and maintain covered information about Nevada consumers who use or visit the online service. The statute excludes from coverage financial institutions subject to the GLBA, entities subject to HIPAA (deviating from the CCPA, which only exempts the personal information collected under those statutes but not the entities themselves), as well as certain motor vehicle manufacturers or repair services.

The Nevada law also defines "**consumer**" more narrowly than the CCPA. Under Nevada law, "consumer" is defined as a person who seeks to acquire any good, service, money or credit for personal, family or household purposes from the operator. Accordingly, SB-220 would likely not apply to the operator's employees nor to business customers who engage with the operator as part of a Business to Business (B2B) relationship.

Finally, the Nevada statute applies to "**covered information**," which is defined as an enumerated list of personally identifiable information about a consumer collected by an operator through a website or online service and maintained in an accessible form, including:

- first and last name;
- home or other physical address;
- email address;
- telephone number;
- social security number;
- identifier allowing contact (physically or online) with a specific person; or
- other information concerning a person that is collected and maintained in combination with an identifier in a form that makes the information personally identifiable.

SB-220's Opt-Out Right

SB-220 requires operators to establish a "designated request address" – via email, toll-free phone number or website – through which a consumer may submit a "verified request" to opt out of the "sale" of any covered information the operator has collected or will collect from a consumer in the future. In this way, SB-220 is less onerous than the CCPA, which requires covered businesses to provide a link – titled Do Not Sell My Personal Information – on the business's website and mobile app, and in the privacy policy.

Operators must verify the authenticity of the request and identify the consumer using "commercially reasonable means." SB-220 does not provide guidance on how such verification should be performed.

Once a verifiable request is submitted by a consumer, operators have 60 days to respond, although this timetable may be extended by up to 30 days if the operator determines an extension is reasonably necessary and provides notice to the consumer.

The obligation to honor the consumer's opt-out request appears to apply indefinitely. Unlike the CCPA, which specifies that a business must honor the consumer's opt-out request for at least 12 months before requesting the consumer reauthorize the sale of personal information, the Nevada statute is silent on the possibility of requesting the reauthorization of data sales in the future.

SB-220's Definition of "Sale"

SB-220's definition of "sale" is far narrower in scope than the CCPA. Under SB-220, a "sale" is limited to "the exchange of covered information for monetary consideration" by the operator to a person who will "license or sell the covered information to additional persons." There are also broad exclusions from the definition of sale, including disclosures:

- to persons who process covered information on behalf of the operator (similar to the service provider exclusion in the CCPA but without the contracting requirements);
- to affiliates that the operator controls, is controlled by, or are under common control with another company;
- for the purposes of providing a product or service requested by a consumer, where the consumer has a direct relationship with the entity to which the data is disclosed;
- for purposes consistent with the reasonable expectations of the consumer, based on the context in which the consumer provided the information; and
- in connection with a merger, acquisition, bankruptcy or other transaction.

This definition is in stark contrast to the definition of "sale" under the CCPA, which includes "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating . . . a consumer's personal information by the business to another business or third party for monetary or other valuable consideration," and which may include some transfers to business affiliates that do not share common branding.

Notice Requirements

SB-220 does not introduce notice obligations beyond what is already required under Nevada law, other than to provide the designated opt-out request address. Nevada's existing online privacy statute requires operators of websites and online services to provide notice on their websites regarding their privacy practices. Such notices must disclose the categories of personally identifiable information collected, categories of third parties with whom the information may be shared, any processes a consumer may use to review and request changes to such information, and whether any third party collects information over time and across different websites or online services.

Attorney General Enforcement

As originally written, SB-220 contained a private right of action. However, the bill was amended to give the Nevada Attorney General's Office sole responsibility for enforcement of both the notice and opt-out requirements, and to specify that there is no private right of action. The attorney general has the ability to impose civil penalties for violations of the statute up to $5,000 per violation.

Takeaways

Nevada was one of more than ten states considering consumer privacy legislation this year – such legislation is still pending in Massachusetts, New York and Rhode Island. The fact that Nevada's opt-out requirement will go into effect in a mere four months (and three months ahead of the CCPA) highlights the need to create privacy and data security compliance programs flexible enough to adapt to quickly evolving state statutory requirements.

Are you ready for the CCPA? Take Orrick's CCPA Readiness Assessment.

- Assess your company against CCPA provisions.
- Receive a complimentary report summarizing the likely key impacts.
- Use the report to develop your CCPA project plan.

---

orrick

Cyber, Privacy & Data Innovation Alert

February 14, 2019

Roller Coaster Start to the New Year for Biometrics: Rosenbach v. Six Flags and Emerging Biometric Laws

by **Aravind Swaminathan** | **David Cohen** | **Nicholas Farnsworth**

A recent decision from the Supreme Court of Illinois heightens the risks faced by companies collecting biometric information by holding that an individual who is the subject of a violation of Illinois' Biometric Information Privacy Act—but who suffered no separate harm from the violation—is an "aggrieved party" with a cause of action under the statute. *Rosenbach v. Six Flags Entertainment Corp., No. 123186 (Ill. Jan. 25, 2019)*. This decision will only further embolden plaintiffs' lawyers to bring biometric privacy suits, and the risk to companies collecting biometric information will likely increase as newly enacted and proposed legislation comes into effect. In this post, we discuss what happened, what is on the horizon, and some steps to consider.

Overview of the Illinois Biometric Information Privacy Act

The Illinois Biometric Information Privacy Act ("BIPA") regulates private entities' (defined broadly) collection, use, storage, and disposal of an individual's "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" (defined as "biometric identifiers") or any information "based on an individual's biometric identifier used to identify an individual" (defined as "biometric information"). BIPA imposes several obligations on private entities in possession of biometric identifiers or biometric information, including requiring:

- the development of a written biometrics retention and destruction policy,
- the disclosure of the content and purposes for which the biometric identifiers or biometric information are collected and used,
- the procurement of a written release for the collection and use of biometric identifiers and biometric information, and
- the implementation of safeguards meeting "the reasonable standard of care within the private entity's industry."

Private entities failing to comply with their obligations under the statute may face litigation based on BIPA's private right of action available to persons "aggrieved" by such statutory violations and could be liable for actual damages or, if greater, "liquidated damages" of $1,000 per negligent violation and $5,000 per intentional or reckless violation of the law.

Preliminary Challenges in Biometric Privacy Litigation

As noted in our last post here, defendants have two separate and independent ways to attack plaintiffs' injury allegations in BIPA and other privacy and cybersecurity litigation:

- challenge the plaintiff's standing through either a federal court Article III challenge[1] or a state court equivalent (which we addressed in more detail in our previous post here discussing the decision from the Northern District of Illinois, *Rivera v. Google, Inc*., 16-02714 (N.D. Ill. Dec. 29, 2018); or
- argue that the plaintiff failed to plead or prove the injury redressable by the cause of action in question (e.g., that the plaintiff was not "aggrieved by a violation" of BIPA).

Rosenbach v. Six Flags Entertainment Corp.

The Supreme Court of Illinois in *Rosenbach v. Six Flags Entertainment Corp*. did not address Article III standing nor the Illinois state court equivalent, but rather focused on the circumstances in which a plaintiff can satisfy the injury requirement contained in BIPA itself—that is, the requirement that the plaintiff be "aggrieved." In *Rosenbach*, a mother filed suit on behalf of her 14-year-old son claiming that the fingerprinting practices of Six Flags, in connection with their repeat-entry pass enrollment process, violated BIPA[2] by collecting the son's fingerprints without informing him or his mother of "the specific purpose and length of term for which his fingerprint had been collected" and without obtaining either his or his mother's written release or consent. In addition to other defenses, Six Flags argued that the plaintiff "had suffered no actual or threatened injury" and, as a result, was not an "aggrieved" person eligible for the BIPA private right of action.

Emphasizing the importance of proper notice and the right to refuse consent, the court explained that "[w]hen a private entity fails to adhere to the statutory procedures . . . 'the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.'" Therefore, the court held that no actual injury, beyond a violation of BIPA, is required for a person to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief.

Takeaways

- The *Rosenbach* decision has several important takeaways for businesses that collect or use personally identifiable information, including biometric identifiers and biometric information:
    - ***Liability risks for alleged mishandling of biometric information are increasing***: Several additional states have laws on the books, or are considering legislation, for biometric information. Although Illinois is currently the only biometric information statute with a private right of action,[3] the risks for entities collecting biometric information are increasing, particularly if other jurisdictions use similar "aggrieved" language and adopt the *Rosenbach* rationale:
    - The California Consumer Privacy Act of 2018 ("CCPA"): The CCPA introduced sweeping changes to the U.S. privacy landscape by granting California residents enhanced rights in relation to their personal information (which includes biometric information), as well as a private right of action for certain breaches of personal information. See here for more information on the latest amendments to the CCPA.
    - The proposed Massachusetts Senate Bill 341: The proposed bill would add a Consumer Data Privacy chapter to the Massachusetts General Laws, which would grant Massachusetts consumers similar rights to those provided under the CCPA in relation to personal information (which may include biometric information). Unlike the CCPA, the proposed bill would create a private right of action for a consumer who has "suffered [any] violation" of the bill and specifically states the intent that a violation of the bill "shall constitute an injury in fact to the consumer . . . and the consumer need not suffer a loss of money or property . . . to bring an action for a violation." See here for a copy of the bill.

- The proposed Washington Privacy Act, Senate Bill 5376 ("WPA"): The proposed WPA would create a new overarching privacy law in Washington State. The proposed law would create an enumerated set of consumer rights in relation to personal data (which includes biometric data) similar to those provided under the CCPA. Although the proposed law does not include a private right of action for aggrieved consumers, a violation of its provisions could result in enforcement by the attorney general. See here for a copy of the bill.

The proposed New York Biometric Privacy Act, Senate Bill 1203 ("BPA"): The proposed BPA would create a new biometric-specific privacy law in New York similar to BIPA. The proposed law would create a private right of action for "[a]ny person aggrieved by a violation" of the statute. See here for a copy of the bill.

- ***Understanding which biometric identifiers/information are collected/used***: Businesses across industries increasingly are (or are considering) using biometrics more frequently, including in relation to:
  - user verification (such as mobile device fingerprint authentication),
  - workforce management (such as fingerprint-based time clocks), and
  - personal identification (such as facial recognition in photographs and video).

With potential liability in private actions or state attorney general enforcement proceedings for mere procedural violations, such as failure to provide adequate disclosure or obtain necessary release/consent, entities using (or considering using) biometrics should take steps to gain a deeper understanding of a business's actual collection, use, storage, and disposal practices relating to biometrics. In that regard, many businesses would benefit from conducting a data mapping exercise and/or information audit to identify the information and practices that would be subject to privacy and cybersecurity laws, such as BIPA. Only with this kind of solid understanding can companies undertake to comply with the patchwork of laws that are emerging and ensure that they are complying with the procedures afforded to avoid the significant litigation risk. Once in place, companies can begin to revise notice, collection, use, and retention practices accordingly. Companies that do not have the resources to undertake a data mapping effort should (at a minimum) understand whether they are collecting biometrics and review privacy policies and terms of service to identify risks and take basic steps to manage them.

- ***Alternative defenses remain***: Despite the *Rosenbach* decision being favorable to plaintiffs, defendants still have other defenses that can be raised in BIPA litigation. These include, but are not limited to:
  - Standing: It remains to be seen whether the Illinois Supreme Court will be open to dismissing BIPA litigation on constitutional standing grounds where the plaintiff suffers no harm apart from the alleged statutory violation. And, as noted above, Article III standing challenges may be viable in federal court.
  - Statutory Interpretation: There are several terms and concepts under the biometric statutes that are still open to interpretation, such as the meaning of "biometric identifiers," what conduct qualifies as the "collection" of biometric information, and whether practices are considered "negligent," "reckless," or "intentional" under BIPA. In addition, businesses may be able to argue that some of their obligations under the statute are satisfied by implicit messaging provided through the context of the process involved in the collection of biometric identifiers or biometric information.
  - Procedural Defenses: Defendants are still able to assert the procedural defenses available to them in all lawsuits, including a failure to meet class certification requirements, improper venue, and lack of personal jurisdiction, among others.

[1] The ability to obtain such a dismissal does not eliminate the risk posed by biometric litigation. If a plaintiff files suit in state court, his or her standing in that court will be determined instead by state standing principles, not

Article III. The plaintiffs from *Rivera* have refiled their claims against Google in the Circuit Court of Cook County, Illinois. *Rivera v. Google LLC*, No. 2019CH00990 (Ill. Cir. Ct.) (to be heard May 24, 2019).

[2] According to the complaint, the fingerprinting process for the repeat-entry passes to the park is as follows: When individuals sign up for repeat-entry passes, Six Flags' system "scans pass holders' fingerprints; collects, records and stores 'biometric' identifiers and information gleaned from the fingerprints; and then stores that data in order to quickly verify customer identities upon subsequent visits by having customers scan their fingerprints to enter the theme park."

[3] The biometrics laws of both Texas (Tex. Bus. & Com. Code Ann. § 503.001) and Washington State (Wash. Rev. Code § 119.375) do not create a private right of action for individuals impacted by an entity's violation of the statutes. However, both statutes grant the attorney general the power to enforce the statutory provisions, including through the imposition of civil fines and penalties.

---

orrick

Cyber, Privacy & Data Innovation Alert

January 2, 2020

The CCPA Is in Effect and It Is Not Too Late to Get Started in 2020

by **Heather Egan Sussman** | **Emily Tabatabai** | **Nicholas Farnsworth** | **Maria Rouvalis**

Happy New Year! At long last, the California Consumer Privacy Act of 2018 ("**CCPA**") went into effect yesterday, January 1, 2020. For those who have not yet heard, the CCPA establishes a comprehensive legal framework to govern the collection and use of personal information, both online and offline, and provides unprecedented privacy rights to California consumers, in effect becoming the *de facto* national standard for U.S. privacy law. The law introduces new legal risks and considerations for companies that collect information from California consumers, due to the law's expansive scope, broad definition of personal information, increased disclosure obligations, enhanced consumer rights, potential for statutory fines and, in the event of a security incident, the potential for consumer class action litigation.

Overview of the California Consumer Privacy Act of 2018

Generally, the CCPA applies to companies that collect and process personal information from or about identified natural persons (i.e., not entities) who are California residents (referred to in the CCPA as "**consumers**"). More specifically, the law applies to any covered "**business**," which is defined as a for-profit sole proprietorship or legal entity that:

- does business in California;
- collects California consumers' personal information (either online, offline or through third-party intermediaries);
- determines the means and method (the why and how) of the processing of personal information; and
- satisfies one or more of the following thresholds:
    1. has annual gross revenues over $25 million; or
    2. derives 50 percent or more of its annual revenues from selling consumers' personal information; or
    3. buys, sells, receives or shares (for commercial purposes) the personal information of 50,000 or more consumers, households or devices annually.

In addition, the law applies to any entity that:

- controls ***or is controlled by*** a CCPA covered "business" (>50% ownership, control of majority of board, or controlling influence over management); ***and***
- ***shares common branding*** with that covered "business" (shared name, service mark or trademark).

Such an entity is also referred to as a "**business**" under the CCPA. The CCPA imposes a number of obligations on covered businesses, including requiring a business to:

- provide detailed disclosures to consumers about the collection, use, disclosure and sale of personal information, as well as the rights available to consumers under the CCPA, in online and, potentially, off-line disclosures ("**Notice to Consumers**").
- provide consumers access to the underlying personal information collected about them and individualized details about their personal information in response to a verifiable request ("**Right to Know**").
- delete personal information the business has collected from the consumer in response to a verifiable request, subject to exceptions ("**Right to Delete**").
- if "**selling**" personal information, add a "Do Not Sell My Personal Information" link to the business's website and mobile application that allows a consumer to opt out of the "**sale**" of personal information ("**Right to Opt Out**").
- not knowingly "**sell**" personal information about a consumer under the age of 16 without proper affirmative authorization or opt-in consent ("**Right to Opt In**").
- not discriminate against a consumer for exercising a right under the CCPA ("**Right to Nondiscrimination**").

The California Attorney General may seek an injunction and statutory civil penalties of up to $2,500 per violation or $7,500 per intentional violation of the CCPA after a 30-day cure period. In addition, the CCPA permits a consumer the right to bring an individual cause of action or a class action against a business if certain nonencrypted or nonredacted personal information is subject to a data breach resulting from a business's failure to implement and maintain reasonable security procedures and practices.

Changes Past, Present and Future

There have been many CCPA-related developments since it was signed into law on June 28, 2018, and more are certain to come in 2020. The first major change occurred on August 31, 2018, with the passing of SB-1121, which amended the CCPA in certain respects, including prohibiting enforcement of the CCPA by the California Attorney General until July 1, 2020, or six months after publication of implementing regulations, whichever is sooner. Given that the final implementing regulations have not yet been published, the enforcement date will be July 1, 2020. Our team summarized the other changes from SB-1121 here.

On October 1, 2019, Nevada stole a bit of the CCPA's thunder by passing its own, much narrower, privacy law amendment addressing the "sale" of personal information. More information about the change in Nevada's law can be found here. California was quick to reclaim the spotlight, with the California Attorney General publishing draft CCPA regulations for public comment on October 10, 2019. The final regulations are yet to be published, but in the meantime please find our team's summary of the proposed regulations here. Lastly, on October 11, 2019, California's Governor signed six CCPA amendments into law, including amendments creating a one-year exception to most of the CCPA's obligations for information relating to a business's personnel and certain information in a B2B context. Please find our team's overview of these comprehensive amendments and their significant impact on CCPA compliance here.

With the law and the recent CCPA amendments all coming into effect yesterday, January 1, 2020, we have much to look forward to in the new year. For starters, the private right of action under the CCPA for certain data breaches is now in effect and we anticipate it won't take long for the plaintiff's bar to jump at the opportunity to try out its new statutory damages. Please find our team's summary of the likely impact of this private right of action here.

In addition, changes to the CCPA are likely to continue as the California Attorney General must still publish its final implementing regulations in advance of the July 1, 2020 enforcement date and additional amendments are likely to be presented in the 2020 California legislative session. The critical personnel and B2B exceptions

described above are also scheduled to sunset on January 1, 2021, so we expect to see at least some early discussion about the long-term prospects for extending or making these exceptions permanent.

Lastly, like we saw in 2019, other states will likely present CCPA-like bills in their own 2020 legislative sessions, and it is more likely these bills will be received positively after a year of discussion. Please find our team's overview of CCPA-like state privacy bills from 2019 here, which very well may be resurrected in 2020.

Takeaway for 2020:

The time to think about CCPA compliance is now, and it is not too late to get started. Taking our CCPA Readiness Assessment is a great first step. Or, feel free to download our Orrick team's PowerPoint, "CCPA Compliance – It's Not Too Late to Get Started!," which covers the critical components of the CCPA and suggests practical ways to begin addressing CCPA requirements. Our Orrick team is here to guide you each step of the way toward CCPA compliance, and we will continue to monitor CCPA developments and share updates here on Trust Anchor.
