Morgan Lewis

PRIVACY CONSIDERATIONS AND THE USE OF COLLECTED DATA

December 11, 2019

Ezra Church
Mark Krotoski
Pulina Whitaker

Table of Contents

Section 01 – Introductions

Section 02 – Overview: How Data is Collected in the Automotive and Mobility Space

Section 03 – Other Emerging Legal Issues

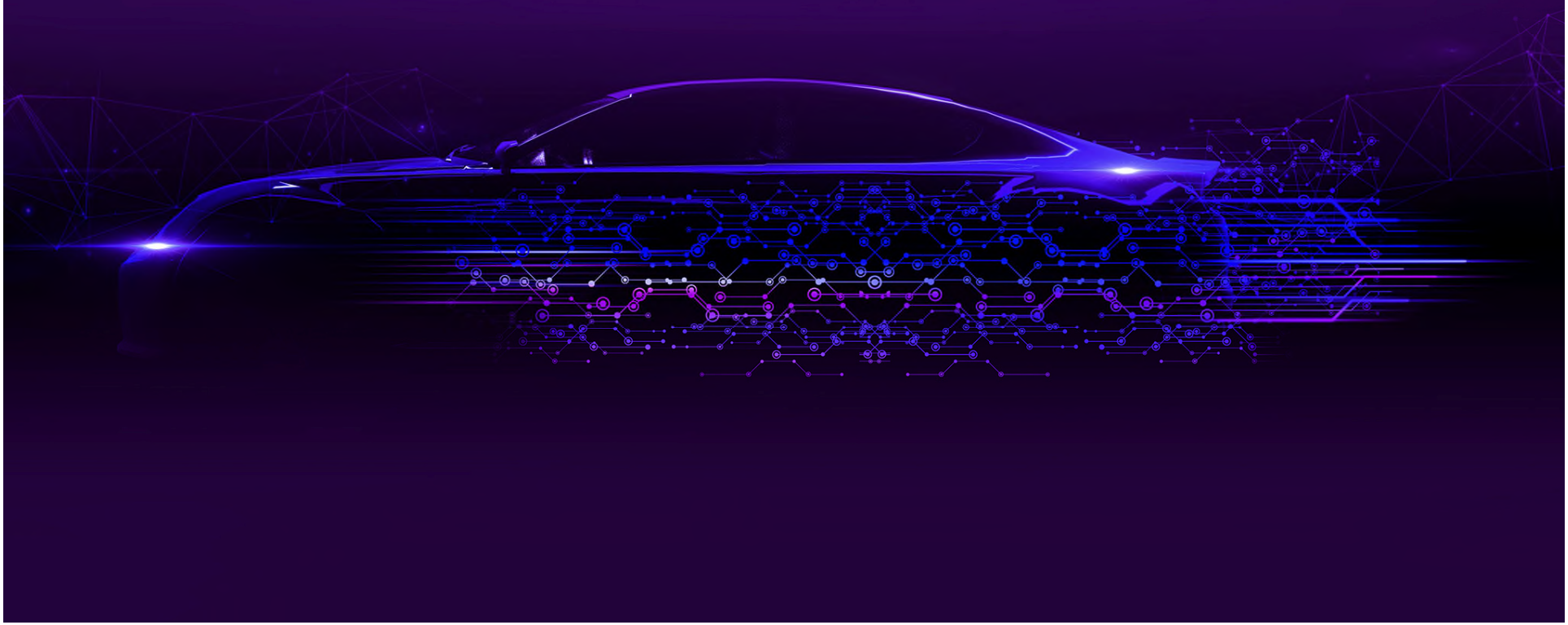
Section 04 – California Consumer Privacy Act

Section 05 – International Implications of Data Collection in Cars

Section 06 – Conclusion

SECTION 01

INTRODUCTIONS



Today's Presenters

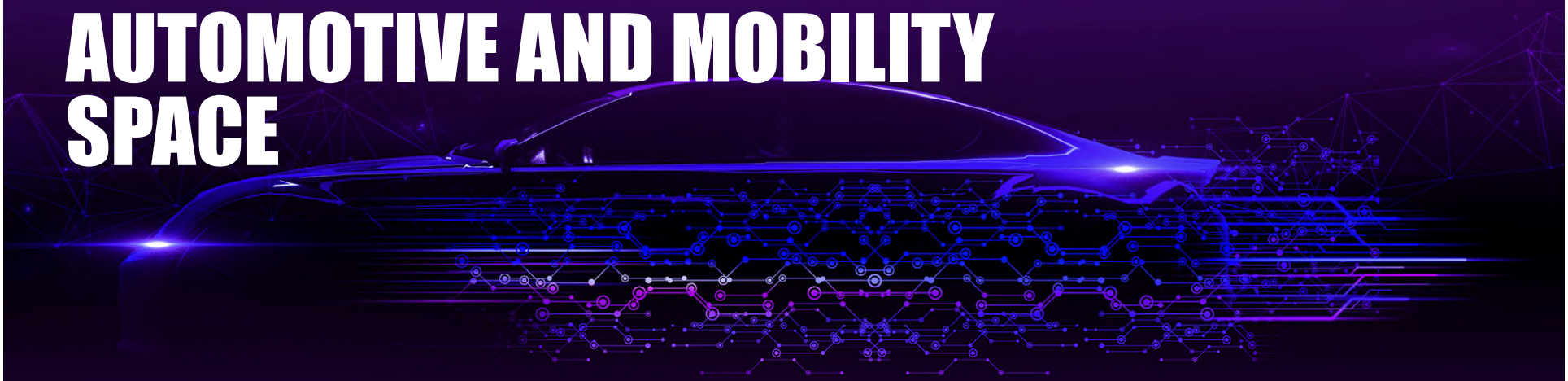
Ezra Church
Philadelphia
Tel +1.215.963.5710
ezra.church@morganlewis.com

Mark Krotoski
Silicon Valley / Washington, DC
Tel +1.650.843.7212
mark.krotoski@morganlewis.com

Pulina Whitaker
London
Tel +44.20.3201.5550
pulina.whitaker@morganlewis.com

SECTION 02

OVERVIEW: HOW DATA IS COLLECTED IN THE AUTOMOTIVE AND MOBILITY SPACE



Connecting Cars and Drivers—Collected Data

- Event Data Recorders—Installed on over 90% of vehicles; technical info about operation in the seconds before and after a crash.
- On-Board Diagnostics—Legally required to have an On-Board Diagnostic port or OBD-II; all vehicles after 1996.
- Location Information—collected by navigation and similar systems.
- External Information—modern vehicles contain cameras and sensors used to gather information about the surroundings.
- In-Cabin Information—microphones, cameras, and other devices.
- User Recognition—systems that recognize physical characteristics, like fingerprint, facial recognition or other biometrics.
- Apps—third-party systems like Apple CarPlay, Android Auto, Pandora, including interface with driver's mobile devices.
- User Mobile Devices—mobile devices themselves may be tracked.

DATA and the CONNECTED CAR

Version 1.0

Today's connected technologies are making transportation safer and more convenient. Many new features are enabled by the collection and processing of data. Cars are becoming part of a trusted mobile ecosystem that ensures data flows between a network of carmakers, vendors and others to support individuals' safety, logistics, infotainment, and security needs. This visual represents devices that may be employed in today's connected cars; no single vehicle will have all of these features, but most new vehicles have some. Much connected car data is protected by technical controls, laws, self-regulatory commitments, privacy policies, and other emerging mechanisms or controls.

Produced by FUTURE OF PRIVACY FORUM
FPF.ORG

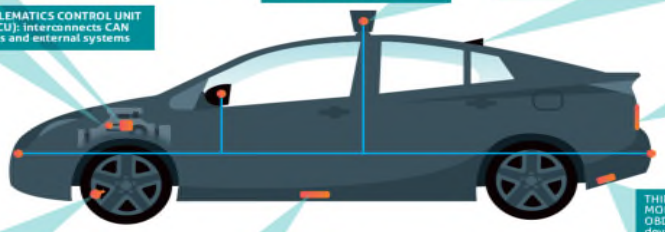
DATA RECEIVERS

A growing number of entities receive and transmit data through the connected vehicle ecosystem

- OTHER CAR (V2V)
- TRAFFIC LIGHT (V2I) & LICENSE PLATE READER
- CAR MAKER
- THIRD PARTIES
- TOLL BOOTH
- EMERGENCY SERVICES
- SATELLITE

WIRELESS CONNECTIVITY

- CELLULAR
- NON-CELLULAR
  - BLUETOOTH
  - WIFI
  - DSRC RADIO
  - SATELLITE/GPS
  - SHORT RANGE RADIO
  - SHORT RANGE RADAR



CAN-BUS: internal communication bridge between Electronic Control Units

TELEMATICS CONTROL UNIT (TCU): interconnects CAN Bus and external systems

AUTONOMOUS VEHICLE IMAGING AND SCANNING: LIDAR, radar, ultrasonic sensors, or exterior cameras

DSRC RADIO: vehicle to vehicle and vehicle to infrastructure communication

License Plate

TIRE PRESSURE SENSORS: short range radio, goes to radio receiver

EVENT DATA RECORDER: black box with accident data

CRASH DATA RETRIEVAL UNIT: extracts EDR data

THIRD PARTY MONITORING DEVICE: OBD-II or external device communicates with fleet operator

RFID VEHICLE TAG: enables short-range tracking

ELECTRONIC TOLL COLLECTION SYSTEM: transponder sends ID via radio

CABIN MONITORING SYSTEM: e.g. monitors eye movement to measure attention

VEHICLE SERVICES: Links to, e.g., roadside assistance and preventative maintenance reminders

GPS UNIT: uses satellite to inform location, navigation

VIN NUMBER: long-used unique vehicle identifier

OBD-II PLUGIN: pulls data from port, or generates own location or movement data

OBD-II PORT: interface to driving and operational data

TOUCH SENSORS: detects driver fatigue through grip, pulse

SIM CARD: connectivity point for transmitting onboard information

WIFI NETWORK: enables in-car internet access

USB PLUG-IN: connects via USB port for power or data transfer

INFOTAINMENT SYSTEM: access entertainment and navigation apps

PHONE- PROJECTING SOFTWARE: mirrors apps from smartphone

SMART PHONE: connects to car via Bluetooth, Wi-Fi or USB

KEY FOB: supports keyless entry

TYPES OF DATA

VEHICLE & SAFETY functioning of vehicle, including maintenance status, mileage, and operations

DRIVER driver physical characteristics or how a person drives a vehicle: i.e. speed, seat belt use, braking habits

LOCATION precise geographic location of a vehicle

ACCOUNT personal accounts established by vehicle owner

Connecting Cars and Drivers—Huge Benefits

- Vehicles are increasingly connected to manufacturers, to their driver's smartphones, and each other.

- Connected cars provide huge promise for enhancing safety, reducing environmental impact, diagnosing malfunctions, calling emergency assistance, improving efficiency and performance, navigation services, providing valuable information, autonomous driving, and more.

Connecting Cars and Drivers—Big Concerns

- But the collection of data in connection with vehicles raise privacy and security concerns:
  - Data security
  - Hacking and safety concerns
  - Collection and use by automakers
  - Collection and use by others (marketing, profiling, investigations, law enforcement, insurance prices etc.)

GAO Report on Vehicle Privacy

- GAO Report, Vehicle Data Privacy, July 2017
- 13 of 16 carmakers offered connected vehicles; all reported collecting, using and sharing data such as location data and operations data
- For all 13, sharing was pretty limited, primarily for research and development
- None reported sharing data that could be linked to a consumer for nonaffiliated or third party use
- Analyzed the privacy policies of 13 automakers

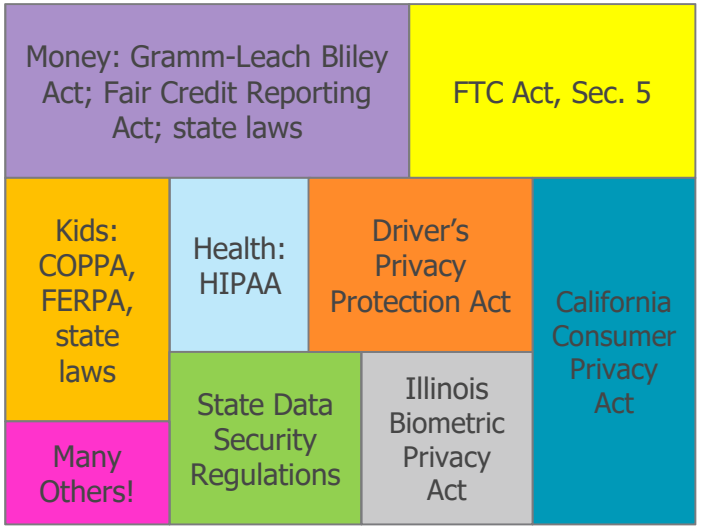
No Comprehensive Privacy Standard for Car Data in the US

Comprehensive v. sector-specific.

EU GDPR

- One comprehensive privacy law
- All industries
- All personal data, regardless of type or context

US Privacy law



Automotive Consumer Privacy Protection Principles

- Industry standard developed in 2014, reviewed against in 2018.
- Designed to establish protection of personal information collected through in-car technology.
- 20 automakers have pledged to meet or exceed the standards.
- Applies to vehicles manufactured starting with the 2017 model year; if compliance requires an engineering change, applies starting with the 2018 model year.

AUTO ALLIANCE
DRIVING INNOVATION℠

Automotive Consumer Privacy Protection Principles (cont.)

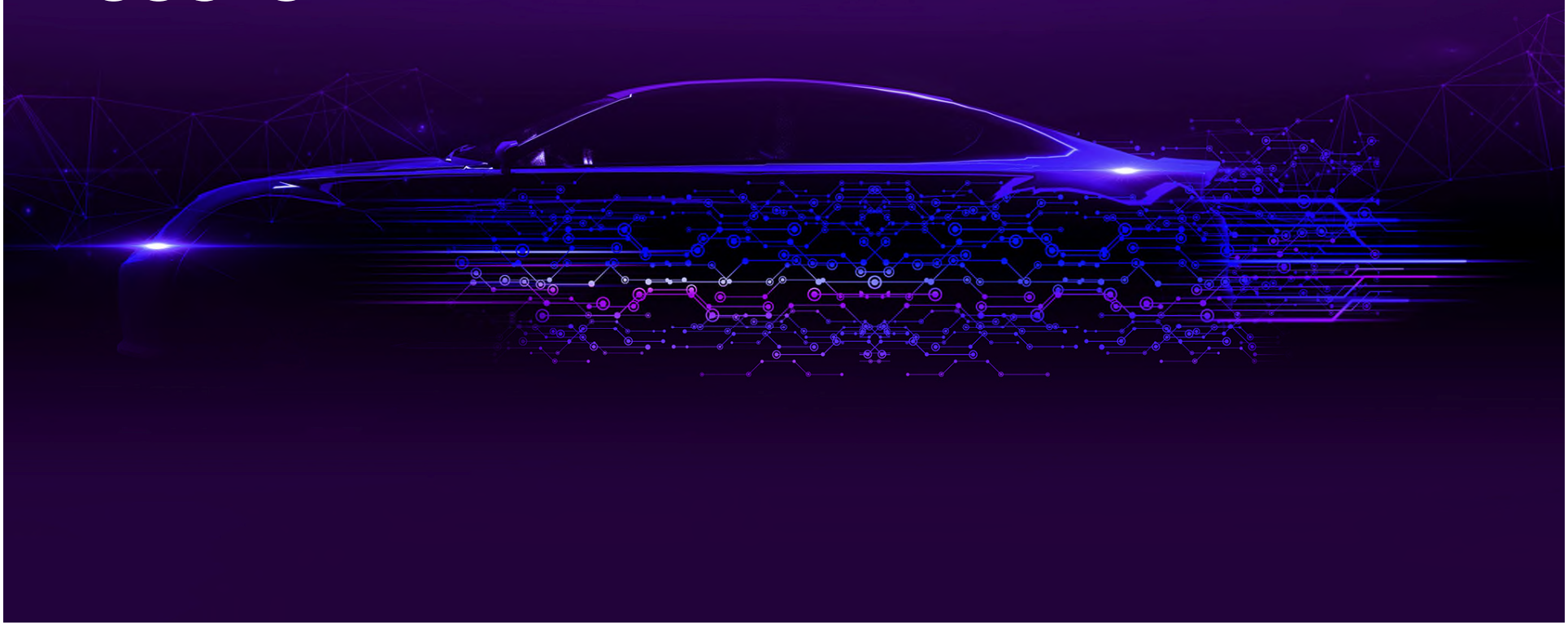
- Transparency: Provide owners and registered users with clear and meaningful information about collection, use, and sharing.
  - Particularly for biometric, geolocation, and driver behavior information.
- Choice: Offering choices regarding collection, use, and sharing.
- Respect for Context: Automakers commit to use and share information consistent with the context in which information was collected and taking into account likely impact on owners and registered users.
- Data Minimization, De-Identification & Retention: Collect information only needed for legitimate business purposes; keep only as long as necessary for legitimate business purposes.

Automotive Consumer Privacy Protection Principles (cont.)

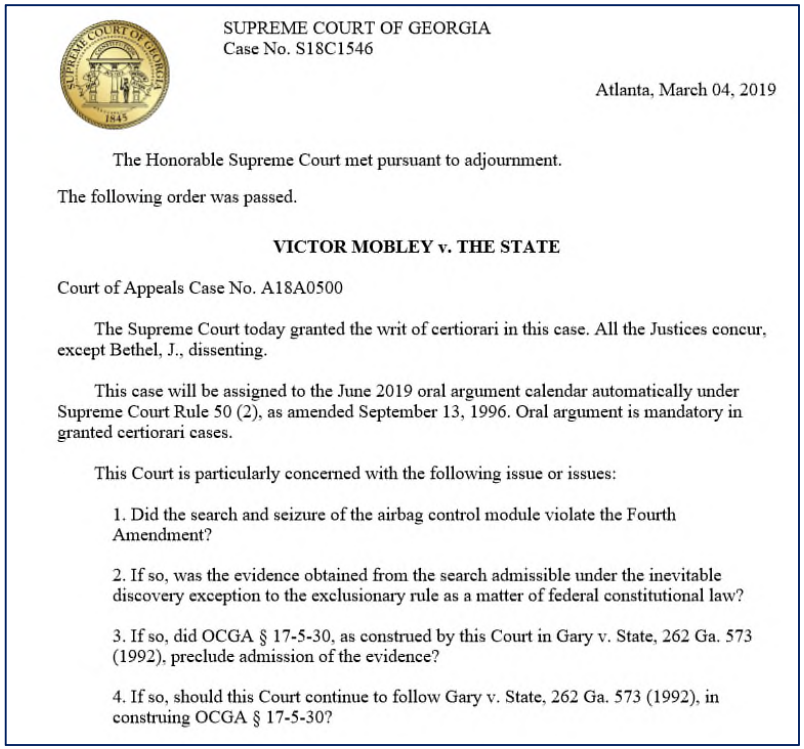
- Data Security: Implement reasonable measures to protect against loss and unauthorized access or use.
- Integrity & Access: Implement reasonable measures to keep information accurate and provide means to review and correct.
- Accountability: Reasonable steps to ensure that they and other entities that received personal information adhere to the Principles.
  - FTC enforcement under Section 5?

SECTION 03

OTHER EMERGING LEGAL ISSUES



Law Enforcement Car Search Issues



SUPREME COURT OF GEORGIA
Case No. S18C1546

Atlanta, March 04, 2019

The Honorable Supreme Court met pursuant to adjournment.

The following order was passed.

VICTOR MOBLEY v. THE STATE

Court of Appeals Case No. A18A0500

The Supreme Court today granted the writ of certiorari in this case. All the Justices concur, except Bethel, J., dissenting.

This case will be assigned to the June 2019 oral argument calendar automatically under Supreme Court Rule 50 (2), as amended September 13, 1996. Oral argument is mandatory in granted certiorari cases.

This Court is particularly concerned with the following issue or issues:

1. Did the search and seizure of the airbag control module violate the Fourth Amendment?

2. If so, was the evidence obtained from the search admissible under the inevitable discovery exception to the exclusionary rule as a matter of federal constitutional law?

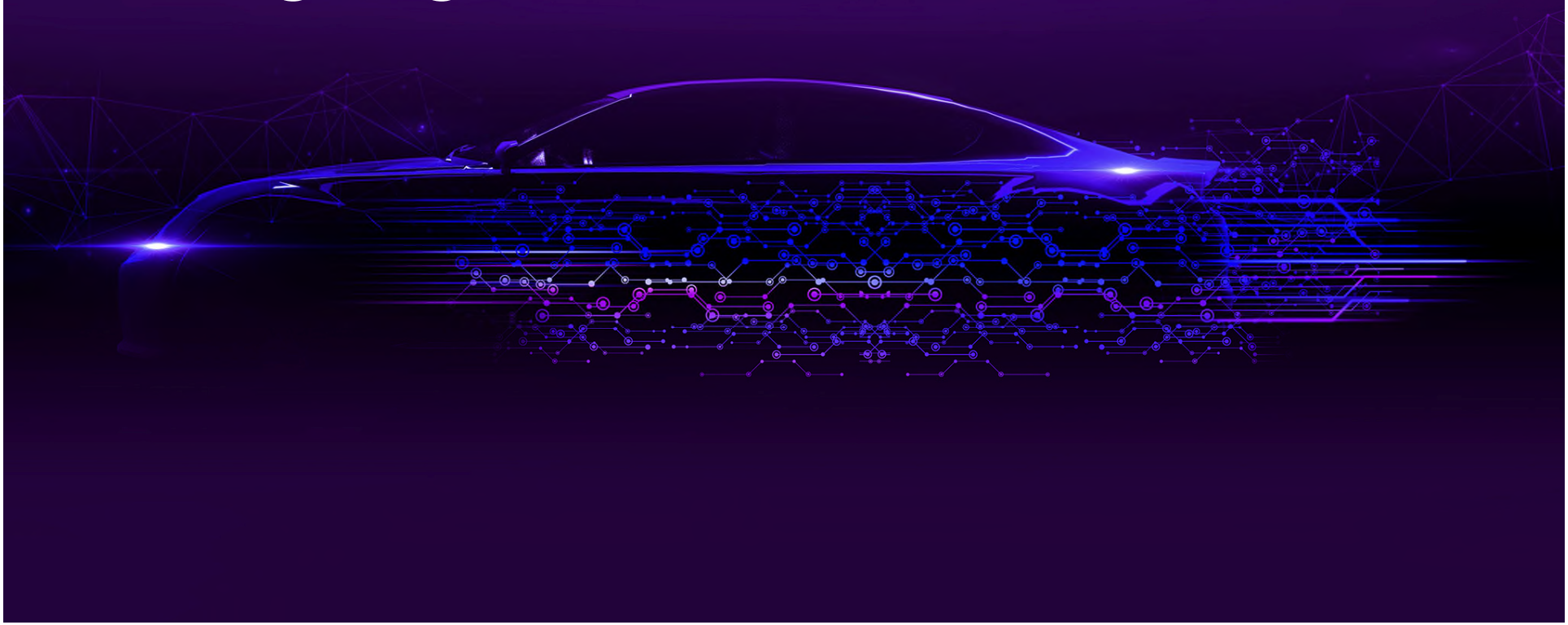
3. If so, did OCGA § 17-5-30, as construed by this Court in Gary v. State, 262 Ga. 573 (1992), preclude admission of the evidence?

4. If so, should this Court continue to follow Gary v. State, 262 Ga. 573 (1992), in construing OCGA § 17-5-30?

https://www.gasupreme.us/wp-content/uploads/2019/03/s18c1546.pdf

SECTION 04

CALIFORNIA CONSUMER PRIVACY ACT



CCPA Landmark Changes

- Timeline
- Coverage
- Broad Definition of "Personal Information"
- New Statutory Rights
- Enforcement / Private Right of Action
- Next Steps

CCPA Timeline

Date	Event
June 28, 2018	CCPA is signed into law
September 23, 2018	SB 1121 amends the CCPA • Extending deadline for issuance of regulations to July 1, 2020 • Enforcement will commence six months after publication of final regulations or July 1, 2020, whichever is sooner
October 10, 2019	AG's office issues Proposed CCPA Regulations • Regulations primarily address consumer privacy rights, and do not address subsequent CCPA amendments, private right of action for security breaches or enforcement
October 11, 2019	Governor signs into law five CCPA amendment bills, which include new exceptions for employee and B2B transaction data • AB 25, 874, 1146, 1355, and 1564
December 6, 2019	Public comment period ends on Proposed CCPA Regulations
January 1, 2020	CCPA takes effect
July 1, 2020	California AG enforcement

Public Review and Comment on CCPA Proposed Regulations

- AG office public hearings on the CCPA draft regulations
  - December 2 in Sacramento
  - December 3 in Los Angeles
  - December 4 in San Francisco
  - December 5 in Fresno
- December 6, 2019:
  - Deadline for submitting written comments on the draft regulations
- Any revision to the proposed regulations will be subject to an additional 15-day comment period.

Factors Influencing the CCPA

- GDPR
  - CCPA is influenced by concepts such as GDPR's "right to be forgotten"
  - GDPR's heightened transparency requirements
  - Right of portability

- CCPA builds upon other unique California privacy laws
  - California Online Privacy Protection Act (CalOPPA)
  - The "Shine the Light" law
  - The "Reasonable security" law

- Reflects recent concerns regarding collection and use of personal information by social media and other tech companies.

Businesses Subject to the CCPA

- For-profit organization or legal entity that:
  - Does business in California
  - Collects consumers' personal information, either directly or through a third party on its behalf
    - "Collects" is broadly defined to include "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means"
  - Either alone, or jointly with others, determines the purposes and means of processing of consumers' personal information
    - Resembles GDPR's "data controller" concept
- Also satisfy one of three thresholds:
  1) The annual gross revenue in excess of $25 million
  2) Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone or in combination
  3) Derives 50% or more of its annual revenue from selling consumers' personal information
- Applies to brick-and-mortar businesses, not just collection of personal information electronically or over the internet
- Does not apply to nonprofits

CCPA Broad Definition of Personal Information

Personal information includes any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household".

1) Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, or passport number
2) Categories of PI described in California's customer records destruction law
3) Characteristics of protected classifications under CA or federal law
4) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
5) Biometric information
6) Geolocation data
7) Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
8) Audio, electronic, visual, thermal, olfactory, or similar information
9) Professional or employment-related information
10) Education information that is subject to the Family Educational Rights and Privacy Act
11) Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

[Cal. Civil Code § 1798.140(o)]

Exclusion for "Aggregated Data"

- Excluded from this definition is "aggregate consumer information"
- Data that is "not linked or reasonably linkable to any consumer or household, including via a device," as well as information that is "publicly available from federal, state, or local government records"
- Gets back to question of anonymization

CCPA Does Not Apply To ....

- Medical information and entities subject to HIPAA or the California Confidentiality of Medical Information Act
- Personal information subject to the Gramm-Leach-Bliley (GLBA) or the California Financial Privacy Act
- Sale of personal information to or from a consumer reporting agency
- Personal information information subject to the federal **Driver's Privacy Protection Act**
- Employee data (new AB 25)
- B2B transaction data (new AB 1355)
- **Vehicle information (new AB 1146)**

Driver's Privacy Protection Act of 1994

- CCPA does not apply to Personal Information "collected, processed, sold, or disclosed" under the federal Driver's Privacy Protection Act of 1994 (18 U.SC. § 2721, *et seq.*)
  - However, this information is not exempt from the private right of action for data breaches, Cal Civ. Code § 1798.145(f).

- DPPA enacted in 1994
  - Protect personal information obtained by state Department of Motor Vehicles
  - Prohibits disclosure or of personal information without the express consent of the person to whom such information applies
  - Limited exceptions (or permissible uses) such use by a court or law enforcement agency, motor vehicle or driver safety and theft, court order, among others

Driver's Privacy Protection Act of 1994

- "Personal Information"
  - "Information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status."

Vehicle information (AB 1146)

- CCPA does not apply to "vehicle information" or "ownership information" "retained or shared between a new motor vehicle dealer, … and the vehicle's manufacturer, … if the vehicle or ownership information is **shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall** …, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose."
- **"Vehicle information"** means the vehicle information number, make, model, year, and odometer reading.
- **"Ownership information"** means the name or names of the registered owner or owners and the contact information for the owner or owners.

Vehicle information (AB 1146)

- A new motor vehicle dealer does not have to delete information that would be used to deal with a vehicle warranty or recall.
  - But the dealer cannot share, sell, or use that data for any other purpose.
- CCPA does not apply to an "activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency…".
  - A credit reporting agency does not have to delete information that it collects about consumers.

New Statutory Rights

- Right to know the categories of information
- Right of access and data portability
- Right to request data be deleted
- Right to opt out of the sale or sharing of personal information to third parties
  - Businesses prohibited from selling personal information of consumers under the age of 16 without explicit consent
- Right to equal service and price

Attorney General Regulation Areas

- Personal information categories
  - "in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns"
- Definition of unique identifiers
- Rules and procedures for consumer opt-out of the sale of personal information
- Business notices and information
- Exceptions necessary to comply with state or federal law
  - including, but not limited to, those relating to trade secrets and intellectual property rights
- "[A]dditional regulations as necessary to further the purposes of this title"

Cal. Civil Code §1798.185(a), (b)

CCPA Requires Many New Privacy Policy Disclosures

- Covered businesses must disclose in online privacy:
  - Consumers' rights to know, delete and opt out of the sale of their information, and
  - How consumers can exercise these rights.
- Proposed regulations confirm that privacy policies must describe a business's practices regarding **online and offline** collection, use, disclosure and sale of personal information.
- Policies must be available in an offline/in-person environment if the business conducts substantial business in such a setting.

Enforcement Avenues

- California Attorney General Enforcement

- Limited Private Right of Action

Attorney General Enforcement

- **Scope**: Civil enforcement for **any violation** of CCPA against a "business, service provider, or other person".
- **Opportunity to Cure**: Applies to violation after business "fails to cure any alleged violation within 30 days after being notified of alleged noncompliance."
- **Civil Enforcement Damages**:
    - Injunctive relief
    - $2,500 for each violation
    - $7,500 for each intentional violation of the CCPA

Attorney General Enforcement

- **Enforcement Delayed**:
  - "[U]ntil six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner."

- **New Consumer Privacy Fund**:
  - Civil enforcement penalties deposited in the Consumer Privacy Fund
  - Intended "to fully offset any costs incurred by the state courts and the Attorney General" in enforcement.

[Cal. Civil Code § § 1798.155(b), 1798.185(c)]

Attorney General Guidance

- "Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title."

Civil Penalties

- **Limited Consumer Private Right of Action**

  (1) Nonencrypted or nonredacted **personal information**

  (2) "subject to an **unauthorized access** and **exfiltration, theft, or disclosure**"

  (3) "as a result of the business's violation of the duty to implement and maintain **reasonable security** procedures and practices appropriate to the nature of the information to protect the personal information"

- **Recovery**
  - Damages
  - Injunctive or declaratory relief
  - "Any other relief the court deems proper"

- **Opportunity to Cure**
  - Statutory Damages

Civil Damages

Statutory or Actual Damages

- **Greater of**:
  - Not less than $100 and not greater than $750 per consumer per incident
  - Or actual damages

Statutory Damages Factors

- Nature and seriousness of the misconduct
- Number of violations
- Persistence of the misconduct
- Length of time over which the misconduct occurred
- Willfulness of the defendant's misconduct
- Defendant's assets, liabilities, and net worth
- Other "relevant circumstances presented by any of the parties"

CCPA New Era in Data Breach Litigation

- **Key Questions**
  - What measures are in place to protect personal information?
  - Can you redact and encrypt where possible?
  - Can you demonstrate there are reasonable security procedures and practices appropriate to the nature of the information to protect the personal information?
  - Are you prepared to respond to an incident?

Next Steps

- Assess what "personal information" is collected based on the CCPA's broad definition
- Review and update privacy policies
- Revise website home pages
- Prepare consumer notifications
- Consider how to verify consumer requests
- Consider safeguarding personal information, including encryption and redaction
- Review and assess "reasonable security procedures" in place to protect personal information

Next Steps (cont.)

- Issue employee privacy notices
- Comply with training requirements
- Review recordkeeping policies and requirements
- If a business collects personal information of minors, special rules apply
- Review non-discrimination issues to provide consumers with the right to equal service and price
- Review and update incident response plans

CCPA Checklist – 14 Steps

CHECKLIST

1. Determine whether the California Consumer Privacy Act (CCPA) applies to your business.

- **A business is only subject to the CCPA if it**
  - Is for profit
  - Does business in California
  - Collects consumers' personal information
  - Determines the purposes and means of processing consumers' personal information
- **In addition, the CCPA only applies to a business that**
  - Has annual gross revenue in excess of $25 million
  - Annually buys, receives for commercial purposes, sells, or shares for commercial purposes personal information of 50,000 or more consumers, households, or devices, or
  - Derives 50% or more of its annual revenue from selling consumers' personal information
- **Exceptions: The CCPA does not apply to**
  - Medical information collected by a covered entity governed by the Health Insurance Portability and Accountability Act (HIPAA) or California Confidentiality of Medical Information Act (CMIA); entities subject to HIPAA or CMIA; or information collected as part of a clinical trial
  - Personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act or California Financial Privacy Information Act
  - Information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994
  - The sale of personal information to or from a consumer reporting agency to be reported in or used to generate a consumer report
  - Efforts to comply with federal, state, or local law; a civil, criminal, or regulatory investigation; or a subpoena or summons
  - Cooperation with law enforcement agencies or exercising/defending legal claims

2. Determine what data elements are collected from California consumers and for what purposes they are used.

- The scope of "personal information" under the CCPA is broad and includes any information that "identifies, relates to, describes, references, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including the following 11 enumerated categories of consumer information:
  1. Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, and passport number
  2. Personal information under California's records destruction law (Cal. Civ. Code § 1798.80(e)), which additionally includes signature, physical characteristics or description, telephone number, insurance policy number, education, employment, employment history, or financial account information
  3. Characteristics of protected classifications under California or federal law
  4. Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies
  5. Biometric information
  6. Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
  7. Geolocation data
  8. Audio, electronic, visual, thermal, olfactory, or similar information
  9. Professional or employment-related information
  10. Education information that is not publicly available personally identifiable information, as defined in the Family Educational Rights and Privacy Act (20 USC § 1232(g), 34 CFR Part 99)
  11. Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
- Excluded from this definition is "aggregate consumer information," which is defined as data that is "not linked or reasonably linkable to any consumer or household, including via a device," as well as information that is publicly available from federal, state, or local government records.

3. Consider how consumers' personal information should be organized.

- Provide required CCPA notices and opt-out and opt-in rights (see steps 4, 5, 10)
- Delete data to comply with the CCPA's right to be forgotten (see steps 4, 5, 8, 9)
- Provide consumer data upon request in a "readily useable format" (see step 6)
- Ensure that agreements with service providers are CCPA compliant (see step 12)
- Train personnel to properly process new requests to exercise privacy rights (see step 11)

4. Revise your website's home page.

- **Right to opt out of sale of personal information to third parties**. Businesses must provide notice to consumers that their personal information may be sold and inform consumers that they have the right to opt out of such sale. In order to comply with this right to opt out, a business must post a "clear and conspicuous link" on its website's home page titled "Do Not Sell My Personal Information," and describe the right and include a link to the "Do Not Sell My Personal Information" page in its privacy policy (see step 5).
- **Right to be forgotten**. Businesses must also inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right. Paths to compliance could include adding instructions in the privacy policy or having a link on the home page

5. Revise your privacy policy.

- **Right to know**. Businesses covered by the CCPA must disclose, at or before the point of collection, in their website privacy policy or otherwise, the following:
  - The categories of personal information to be collected about the consumer and the purposes for which the information will be used
  - The categories of consumers' personal information that were actually collected in the preceding 12 months and sold or disclosed for business purposes in the preceding 12 months
- **Right to be forgotten**. Businesses must also inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right, but one of the best paths to compliance would be to add such a provision to the privacy policy.
- **Right to opt out of sale of personal information to third parties**. As mentioned in step 4, in order to comply with the right to opt out, a business must describe the right and include a link to the "Do Not Sell My Personal Information" page in its privacy policy.

6. Create a process and identify individuals responsible for preserving copies of "specific pieces of personal information that the business has collected about [each] consumer" and promptly responding to consumers' requests to access same.

- Such information must be delivered free of charge to a consumer within 45 days, by mail or electronically.
- Information provided pursuant to a request must be portable, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity "without hindrance."
- There is an exception for personal information that is collected for "single, one-time transactions."

7. Create a documented process (including, but not limited to, a toll-free number and website address) and identify individuals responsible for responding to "verifiable consumer requests" with individualized disclosures about the business's collection, sale, or disclosure of the personal information belonging to the specific consumer making the request.

- Businesses must make available two or more designated methods for the consumer to request this information, including, at a minimum, a toll-free telephone number and website address (if the business maintains a website).
- Consumers have the right to make such requests twice in any 12-month period.
- In response to such requests, the CCPA requires businesses to disclose
  - The categories of personal information the business collected about the consumer
  - The categories of sources from which personal information is collected
  - The business or commercial purpose for collecting or selling personal information
  - The categories of third parties with whom the business shares personal information
  - The specific pieces of personal information the business has collected about the consumer
  - The categories of the consumer's personal information that were sold or disclosed for business purposes in the 12 months preceding the consumer's verifiable request

8. Create policies that reconcile the CCPA's requirement to delete data upon request with the need to preserve evidence in litigation and avoid sanctions for spoliation of evidence.

9. Create a process and identify individuals responsible for deleting consumer data in response to such a request.

- Exceptions to such requests include where retention of the consumer's personal information is necessary to
  - Complete a transaction for which the personal information was collected, provide goods and services to the consumer, or otherwise perform a contract with the consumer
  - Detect security incidents, fraud, or illegal activity
  - Exercise free speech, or ensure the right of another consumer to exercise his or her right of free speech
  - Enable internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business
  - Comply with a legal obligation
  - Otherwise use the consumer's personal information internally and in a lawful manner that is compatible with the context in which the consumer provided the information

10. Provide minors with a "right to opt in."

- Businesses are prohibited from selling personal information of consumers between the ages of 13 and 16 without first obtaining affirmative opt-in consent (1) from the consumer or (2) from a parent or guardian where the consumer is under the age of 13.

11. Provide training for employees on the CCPA's prescribed consumer rights.

- Businesses must ensure that personnel responsible for handling consumer inquiries regarding these new privacy rights are informed of the applicable requirements and know how to direct consumers to exercise those rights.

12. Review existing agreements with third parties or service providers to ensure that contracts limit the service provider's use of personal information as strictly as the CCPA prescribes, and revise as needed.

- The CCPA allows businesses to share personal information with third parties or service providers for business purposes, so long as there is a written contract prohibiting the third party or service provider from selling the personal information or "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."
- The CCPA defines "business purpose" as "the use of personal information for the business's or service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected." The CCPA enumerates categories of activities that constitute "business purposes," including auditing; detecting security incidents; performing services, such as maintaining or servicing accounts, providing customer service, processing payments, fulfilling orders and transactions, and providing analytic services; and undertaking internal research for technological development and demonstration.
- Without a CCPA-compliant service provider agreement, the disclosure of personal information to a vendor may constitute a sale of personal information that triggers the consumer's opt-out right.

13. Provide consumers the right to equal service and price.

- Prohibits businesses from discriminating against consumers who exercise their rights under the CCPA.
- A business is specifically prohibited from
  - Denying goods or services to a consumer
  - Charging a consumer a different price or rate for goods or services including through the use of discounts or other benefits
  - Imposing penalties on a consumer
  - Providing a consumer with a different level of quality or service
  - Suggesting a consumer will receive a different price or rate or different level of quality of goods or services

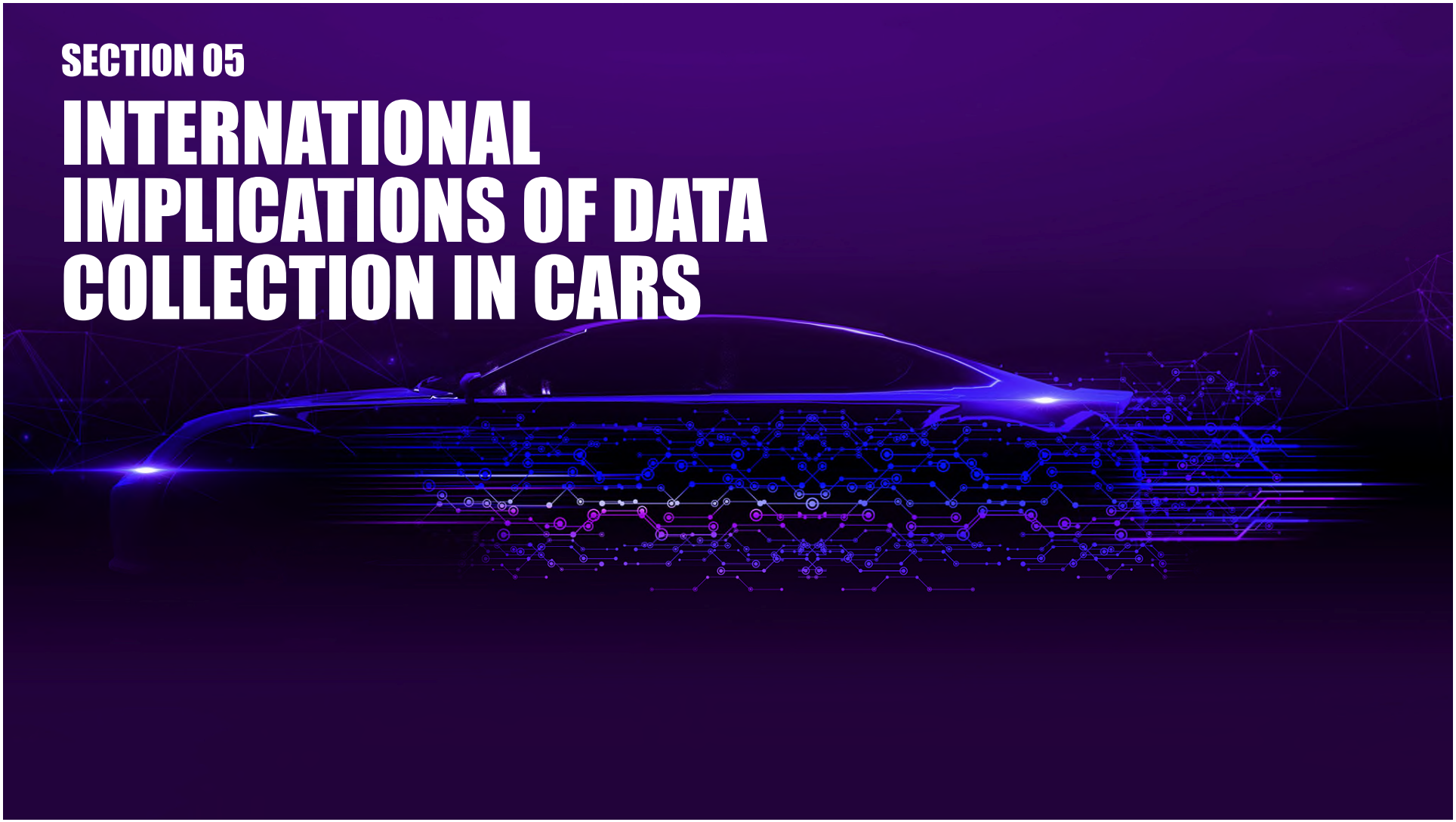
14. Create and maintain a robust incident response plan.

- While implementing a robust incident response plan has been a best practice for some time, the CCPA's new statutory damages and civil penalties further underscore the need for a thoughtful and comprehensive approach to breach response because the act will almost certainly lead to a spike in data breach-related litigation in California.

Morgan Lewis

SECTION 05

INTERNATIONAL IMPLICATIONS OF DATA COLLECTION IN CARS



European data privacy

- GDPR: identifiable data processing restrictions
- Privacy by design requirements
- Data transfer restrictions
- Rights to control personal data processing
- Data security incidents – do you need to report?

Personal data processing

- Data generated will be personal where an individual is identifiable or identified e.g. vehicle owner or driver
- It will be pseudonymised if steps taken to de-identify but not anonymous unless irreversibly de-identified
- Need a lawful processing ground e.g. legal, contractual or legitimate interests
- Transparency of personal data processing is required
- Privacy by design/default required under GDPR

The GDPR – Key Changes

- Data subject rights of access and rights to restrict or erase data and rights of portability – within one month (or up to three months); no fee
- Stricter processing requirements for special categories of data e.g. health information or biometrics:
  - express, informed, freely given consent
  - employment laws
  - assessment of working capacity
- Data protection impact assessment: required prior to processing if high risk for individuals
- Penalties for breach of GDPR – up to higher of 4% global turnover or €20,000,000 (depends on nature and extent of breach)
- Controllers and processors directly liable under GDPR
- Processor audit rights required by controllers
- Record keeping requirements
- DPO
- Appointed representative

Privacy by design/default

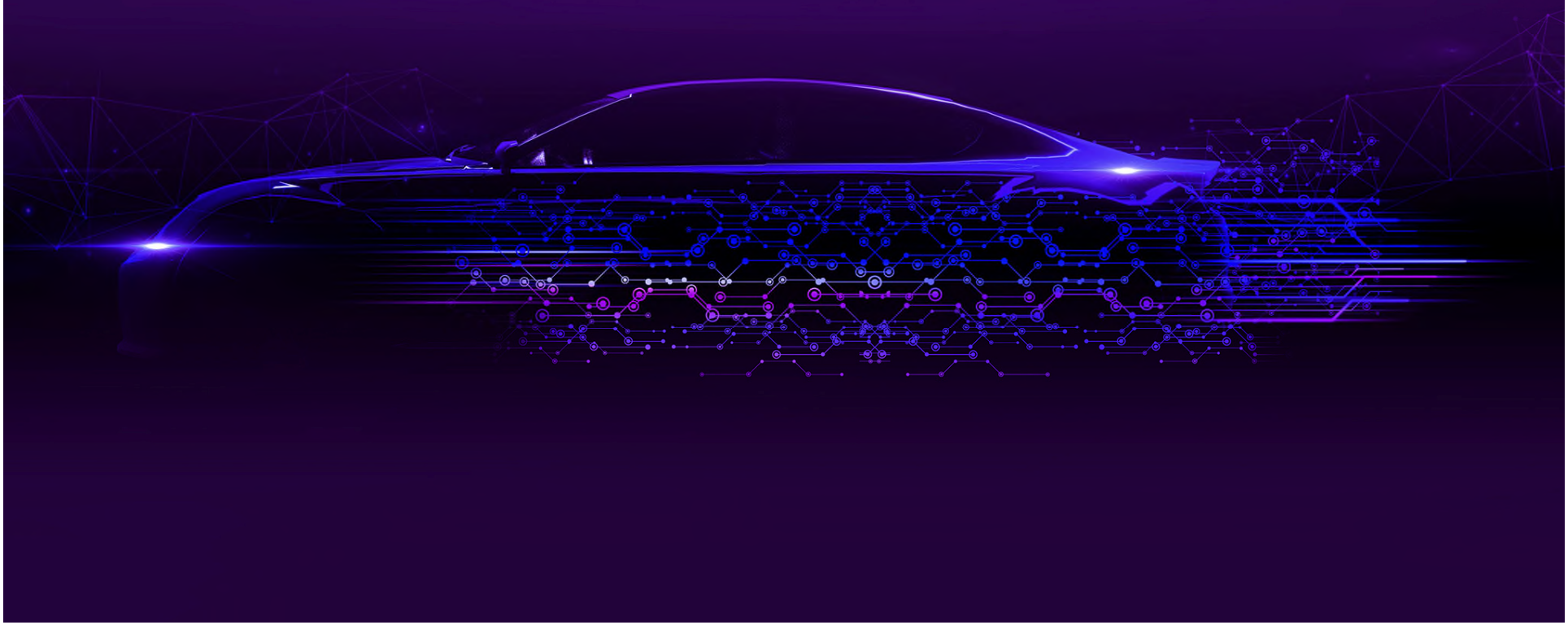
- GDPR requires controllers to implement "technical and organisational measures" to implement data protection principles e.g. data minimisation
- Certification mechanisms likely to be useful to demonstrate compliance with benchmark practices as market evolves
- Complaints for data processing likely to include lack of privacy by design/default

Remedies

- High fines: higher of up to 4% global annual turnover or EUR 20 million
- Regulatory investigations or audits
- Damages even where no financial loss suffered
- Controllers vs processor liabilities
- Class actions/group action remedies in Europe

SECTION 06

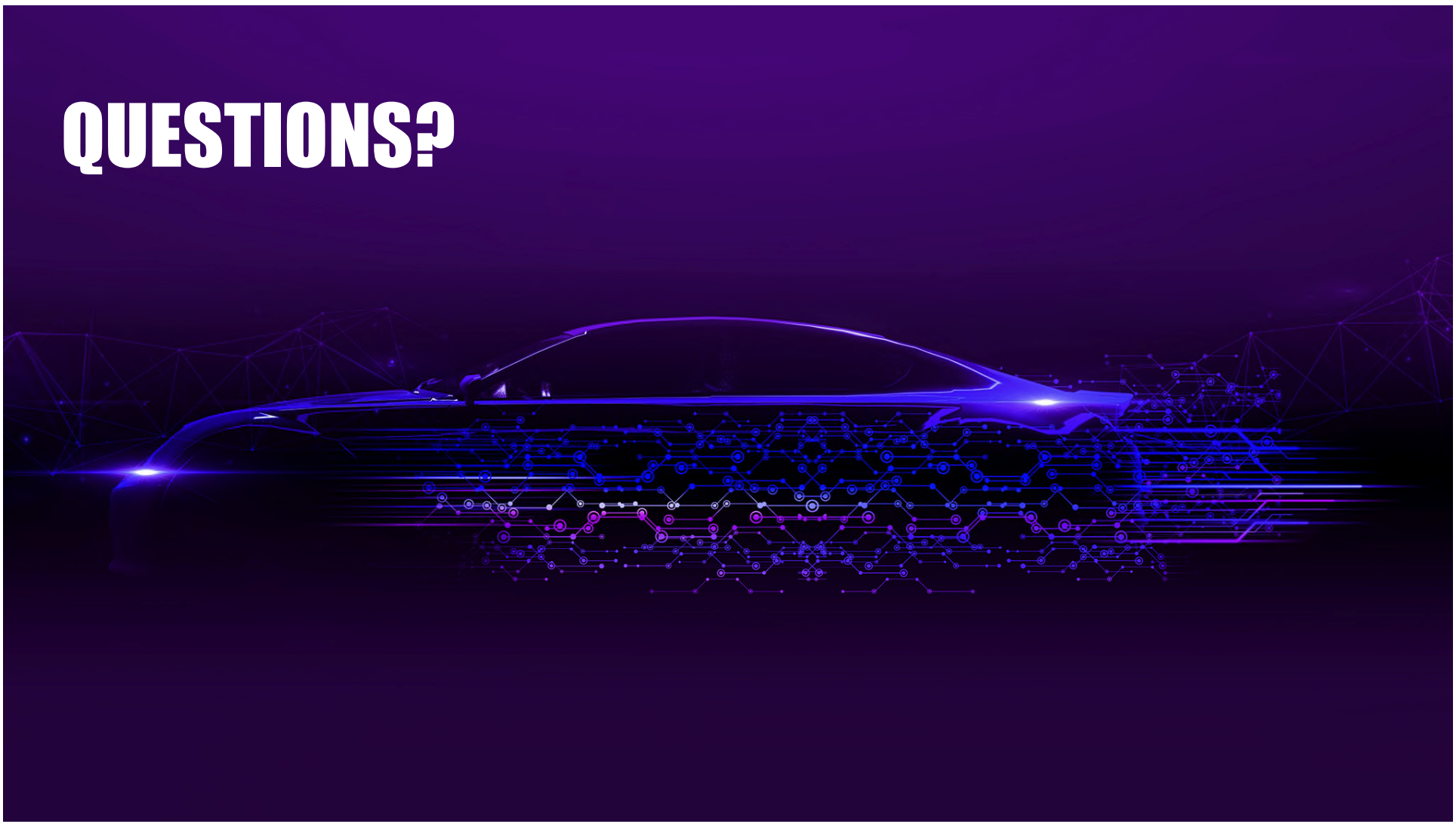
CONCLUSION



Conclusion

- Evolving technology with huge consumer benefits and significant risks
- Evolving standards as law struggles to respond
- Industry principles stand in the gap
- Watch application of CCPA (and potential other state laws) and the GDPR

QUESTIONS?



Biography

Ezra D. Church
Philadelphia
+1.215.963.5710
ezra.church@morganlewis.com

Ezra D. Church focuses his practice on privacy and data security matter. His work includes representation of companies faced with privacy class actions, government investigations, and he has advised hundreds of companies in connection with data breaches and privacy and cybersecurity compliance issues such as data transfer, privacy policies and notice, information security policies, and online and mobile data collection. He writes and speaks frequently on these topics. Ezra has been designated a Certified Information Privacy Professional (CIPP) with the International Association of Privacy Professionals (IAPP).

Biography

Mark L. Krotoski
Silicon Valley | Washington, DC
+1.650.843.7212
+1.202.739.5024
mark.krotoski@morganlewis.com

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues
- Co-Leader of Privacy and Cybersecurity Practice
- Advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Experience handling complex and novel cyber investigations and high-profile cases
    - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
    - Served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, in addition to other DOJ leadership positions.

Biography

Pulina Whitaker
London
+44.20.3201.5550
pulina.whitaker@morganlewis.com

Pulina Whitaker's practice encompasses both labour and employment matters as well as data privacy and cybersecurity. She manages employment and data privacy issues in sales and acquisitions, commercial outsourcings, and restructurings. Pulina provides day-to-day advisory support for multinationals on all employment issues, including the UK's Modern Slavery Act and gender pay reporting requirements. She also advises on the full spectrum of data privacy issues, including preparing for the General Data Protection Regulation. Pulina has deep experience managing international employee misconduct investigations and has been appointed as a Compliance Monitor for the United Nations.

She has been described by clients in The Legal 500 as "extremely knowledgeable with a practical approach" and is noted as being "a key name for issues covering employment and data privacy work."

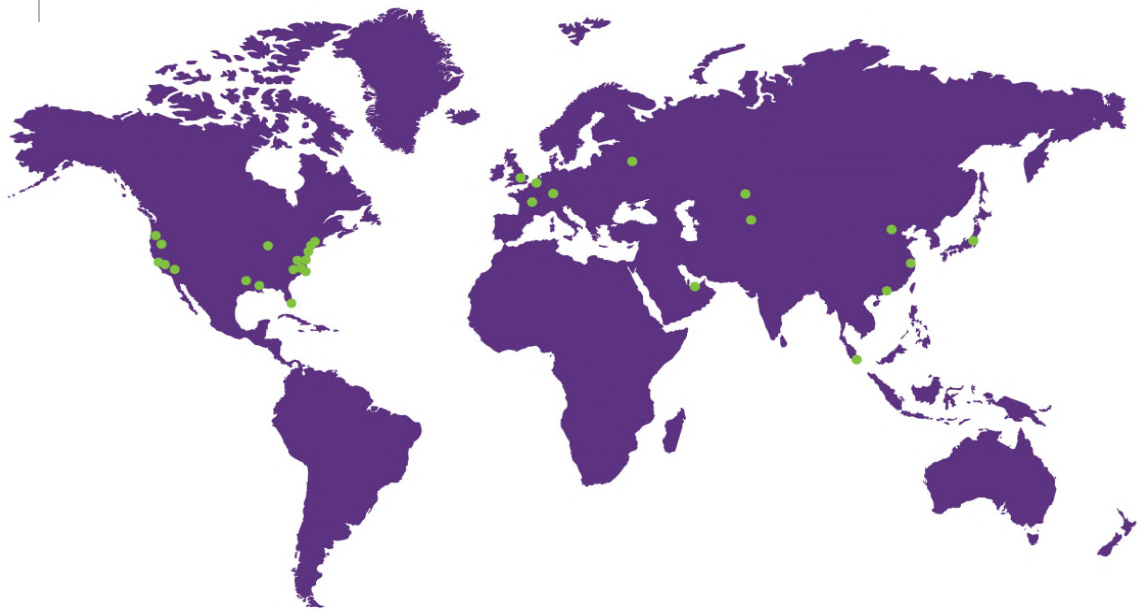
THANK YOU

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.