

Preparing for the California Consumer Privacy Act

What You Need to Know and Do Now

Stephanie Duchene

Partner, Los Angeles

+1 213 220 5176

SDuchene@mayerbrown.com

Lei Shen

Partner, Chicago

+1 312 701 8852

Lshen@mayerbrown.com

Kendall Burman

Counsel, Washington DC

+1 202 263 3210

KBurman@mayerbrown.com

Speakers



Stephanie Duchene, *Partner* (Los Angeles)

Stephanie Duchene is a partner in Mayer Brown's Los Angeles office and a member of the Insurance group. She focuses her practice on representing insurance companies, producers and other insurance licensees and insurance-related service providers in complex and sensitive regulatory matters, including negotiating and resolving significant single and multi-state examinations and investigations, counseling clients on compliance with licensing, claims handling, marketing and advertising rules, and advising clients on the development of new insurance products from initial concept through regulatory approval and into the market. She advises clients on all lines of insurance, including accident, life and health, property and casualty, as well as surplus and excess lines. Additionally, she regularly counsels insurtech companies, traditional carriers and non-insurance entities on the intersection of insurance law and innovation in the industry.



Lei Shen, *Partner* (Chicago)

Lei Shen is a partner in the Cybersecurity & Data Privacy and Technology Transactions practices in Mayer Brown's Chicago office. Lei advises clients regarding a wide range of global data privacy and security issues. She advises companies on navigating and complying with state, federal, and international privacy regulations, including with regard to global data transfers, data breach notification, the California Consumer Privacy Act (CCPA), the EU General Data Protection Regulation (GDPR), the Children's Online Privacy Protection Act (COPPA), CAN-SPAM, and more. She also advises on e-commerce issues, such as electronic contracting and signatures, and on issues concerning mobile privacy and emerging technologies, such as telematics services, Internet of Things, and big data.



Kendall Burman, *Counsel* (Washington DC)

Kendall Burman is a Cybersecurity & Data Privacy counsel in Mayer Brown's Washington DC office. Kendall advises a broad range of clients, including financial services and technology companies, on legal, regulatory, and policy issues involving emerging technologies, security, privacy, and the flow of information across borders. Her practice focuses on advising clients on their privacy and data security policies and practices, including advising companies on how to develop their information programs in ways that comply with the law and industry best practices. Kendall also advises and advocates for clients on new and complex policy and compliance issues involving big data, artificial intelligence, and other technologies.



This presentation provides information and comments on legal issues and developments of interest to our clients and other friends. It is not a comprehensive treatment of the subject and is not intended to provide legal advice. Please seek legal advice before taking any action on the matters discussed here.



Agenda

1. Origin Story
2. Essential Components of the CCPA
3. Requirements of the CCPA
4. Tricky Aspects
5. Exemptions and Enforcement
6. Further Changes on the Horizon
7. Practical Steps Towards Compliance

How did we get here?

The origin story behind the CCPA

California Consumer Privacy Act (CCPA): How We Got Here



1972 California Constitution amended to include the right of privacy as an “inalienable” right



Between 1972 and 2018 California adopted numerous privacy laws, including Online Privacy Protection Act, Privacy Rights for California Minors in the Digital World Act, Shine the Light, and Data Breach Law



In March 2018 the Cambridge Analytica scandal highlighted potential privacy abuses domestically and abroad



In May 2018 California for Consumer Privacy announced it had obtained sufficient signatures to place the California Consumer Privacy Act on the November 2018 ballot

CCPA – Procedural Posture



Passed, signed on June 28, 2018 as a compromise between activists and industry



Legislature began amending almost immediately; multiple amendments passed legislature in September 2018 and await Governor's signature



AG held public forums earlier in the year and we await the regulations (expected October 2019)



- Considered to be the most sweeping privacy law in US
- Effective on January 1, 2020
- AG enforcement likely not until July 1, 2020
- Other states possibly following suit
- New ballot initiative proposed

Who and what does the CCPA apply to?

Focus on CCPA definitions

Key Definitions



Business



Consumer



Personal
Information
(PI)



Who Does the CCPA Apply to?

Applies to “businesses” that collect (or determine the purposes and means of processing)
“consumer” “personal information”

CCPA—Definitions and Scope

Business Definition, Part 1

A “business” is defined as:

- Any sole proprietorship, partnership, LLC, corporation, association or “other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners” that:
 - Collects consumer PI or determines the “purposes and means of the processing of” PI either alone or jointly with others
 - Conducts business in California
 - Satisfies one of the following thresholds:
 - Gross revenue threshold: gross revenues in excess of \$25 million USD, as adjusted
 - Collection threshold: buys, receives, sells or shares PI of 50,000 or more consumers, households or devices
 - Sale threshold: derives 50 percent or more of its annual revenues from “selling” consumer personal information

CCPA—Definitions and Scope

Business Definition, Part 2

However, a “business” can *also* be:

- Any entity that controls or is controlled by a business as defined in Part 1 of the definition and that “shares common branding with the business”
 - “Control” or “controlled” means:
 - “Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business”
 - “Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions”
 - “Power to exercise a controlling influence over the management of a company”
 - “Common branding” means a “shared name, service mark, or trademark”

CCPA—Definitions and Scope

Consumer Definition

A “consumer” is defined as:

- Natural person who is a California resident (as defined in Section 17014 of Title 18 of California Code of Regulations)
- Much broader than definition of consumer under other privacy laws which typically require a transactional nexus
- Applies even to California residents that do not seek a product or service from your company

CCPA—Definitions and Scope

Personal Information Definition

“Personal information” is defined as:

- Information that “identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”
- Does not include “publicly available information” made available from government records
- Does not include deidentified or aggregated information (clarified by AB 874)
- Does not include employment related information (AB 25) or business contact information (AB 1355)
- Expansive definition – far broader than prior privacy laws

CCPA—Definitions and Scope

Personal Information Definition

- Includes but is not limited to the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household:
 - **Identifiers:** real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver’s license number, passport number, or similar
 - Any category of PI described in Civ. Code § 1798.80(e)
 - Characteristics of protected classifications under California or federal law
 - **Commercial information**, including records of personal property, products or services purchased, obtained or considered or other purchasing or consuming histories or tendencies
 - **Biometric** information
 - **Internet or other electronic-network activity information**, including but not limited to browsing history, search history and information regarding a consumer’s interaction with a website, application or online advertisement
 - **Geolocation** data
 - Audio, electronic, visual, thermal, olfactory or similar information
 - **Professional or employment-related information**
 - **Education information**, defined as information that is not publicly available personally identifiable information as defined in Family Educational Rights and Privacy Act (FERPA)
 - **Inferences** drawn from any information identified in this subdivision to create a profile about a consumer reflecting preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes



What is a Sale under the CCPA?

The CCPA creates a number of consumer rights and corresponding business obligations if a business is *selling* a consumer's personal information

CCPA—Definitions and Scope

Definition of Sale

A “sale” is defined as:

- Selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration

A business does not sell personal information when:

- A consumer uses or directs the business to disclose the information to a third party
- The business shares the information with a service provider to perform a business purpose
- The business transfer information to a third party as part of a merger, acquisition, bankruptcy, etc.

CCPA—Definitions and Scope

Definition of Service Provider

A “service provider” is defined as:

- A legal entity that processes information on behalf of a business and to which the business discloses personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business
- Various contractual requirements for a vendor to be considered a “service provider” under the CCPA
- See also definition of “third party” and definition of “sale” for additional service provider requirements

What does the CCPA require?

Recognizing individual rights in consumer personal data

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
<p>Right to Know</p> <p>Right to know business's data practices.</p>	<ul style="list-style-type: none"> • <i>At or before point of collection</i>, inform consumers as to the categories of PI collected and purposes for which PI shall be used • Privacy policy, California-specific description of consumer privacy rights, or website must: <ul style="list-style-type: none"> • List categories of PI collected / sold / shared about consumers in preceding 12 months by reference to enumerated categories listed in definition of PI • Disclose sources from which PI is collected, the business or commercial purpose for collecting/selling PI, categories of third parties with whom business shares PI
<p>Right to know what consumer's rights are under the CCPA.</p>	<ul style="list-style-type: none"> • Privacy policy, California-specific description of consumer privacy rights, or website must: <ul style="list-style-type: none"> • Describe consumer's rights under the CCPA, including right to know, right to deletion, right to opt out, right against discrimination and designated methods for submitting requests for information

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
<p>Right to Access</p> <p>Right to request the business disclose:</p> <ul style="list-style-type: none"> • categories <u>and specific pieces</u> of PI collected • categories of sources from which PI was collected • the categories of PI the business sold / categories of third parties to whom sold • categories of PI disclosed for a business purpose • business purpose for collecting/selling PI 	<ul style="list-style-type: none"> • Make available two or more designated methods for submitting consumer request, including a toll-free telephone number; businesses that operate exclusively online and have a direct relationship with consumer can provide a designated email address instead of telephone number (AB 1564) • Disclose and deliver requested information “free of charge” within 45 days of “receiving verifiable consumer request” looking back 12 months • Must “promptly” take steps to determine whether consumer request is from a “verified consumer” but this will not extend the 45 days; authentication should be reasonable in light of the nature of the personal information requested and may deny requests if unable to verify (AB 25) • Disclosure must be made in writing and delivered through consumer’s account, if maintained (business may not require creation of account), or by mail or electronically at the consumer’s option; in a readily usable format • PI collected / sold / shared must be disclosed by reference to the categories listed in the definition of PI that most closely describe it • If business has not shared or sold consumer's PI in last 12 months, it must disclose this fact

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
<p>Right to Opt Out</p> <p>Right to opt out of sale of personal information to a third party</p> <p>“Sell” includes “releasing, disclosing, transferring, or otherwise communicating” a consumer’s PI to another business or third party “for monetary or other valuable consideration”</p> <p>Minors: Affirmative consent to sale required for consumers 13-16 years old; affirmative consent from parent/guardian required for consumers under 13 years old</p>	<ul style="list-style-type: none">• Must respect consumer’s decision to opt out of sale of PI for at least 12 months before requesting re-authorization of sale• If business “sells” PI, it must provide “clear and conspicuous link” on homepage titled “Do Not Sell My Personal Information” that directs to opt-out website• Must include description of right to opt out along with separate link to “Do Not Sell My Personal Information” page in privacy policy/California rights page• Must ensure all individuals responsible for handling consumer inquiries about business’s privacy practices or compliance with the CCPA are informed of consumer’s right to opt out and how to direct consumers to exercise right• A sale does not occur when:<ul style="list-style-type: none">– Business transfers PI to a third party as an asset that is part of a transaction in which the third party assumes control of all or part of the business– When PI is disclosed to a “service provider”

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
<p>Right to Delete</p> <p>Right to compel business to delete PI that has been collected</p>	<ul style="list-style-type: none"> • Must delete consumer’s PI from records and direct any service providers to delete the consumer’s PI from their records • Numerous exceptions – not required to delete PI if needed to: <ul style="list-style-type: none"> – Complete the transaction for which the PI was collected – Comply with a legal obligation – Detect security incidents / protect against illegal activity – Enable solely internal uses that are reasonably aligned with consumer’s expectations – Otherwise use the PI internally in a lawful and compatible manner
<p>Anti-Discrimination</p> <p>Right for consumer not to be discriminated against for exercising CCPA rights</p>	<ul style="list-style-type: none"> • Cannot discriminate against consumer because consumer exercises CCPA rights, such as: <ul style="list-style-type: none"> – Denying goods or services to consumer – Charging different prices or rates for goods or services – Providing a different level of goods or services to consumer – Suggesting that consumer will receive different price, rate or quality for goods or services • May charge a consumer a different price/rate or provide a different level/quality of service if that difference is reasonably related to the value provided to the business by the consumer’s data. (AB 1355)

CCPA Creates Significant New Privacy Rights and Corresponding Business Obligations

Consumer Rights	Business Obligations
<p>Private right of action</p> <p>Consumers whose nonencrypted or nonredacted information is subject to a data breach as a result of the business's violation of its duty to implement and maintain reasonable and appropriate security procedures may institute a civil action.</p>	<ul style="list-style-type: none">• Encrypt or redact stored information• Implement and maintain reasonable security procedures • Subject to damages:<ul style="list-style-type: none">– Injunctive/declaratory relief– Actual or statutory damages of \$100-\$750 per consumer per incident, whichever greater– Consumer must provide business 30 days' written notice and time to cure • GLBA exemption does not apply to this right; exemptions for employee information and business contact information do not apply to this right

Digging deeper:

Tricky Aspects of the CCPA



“Look Back” Period

- Businesses must disclose and deliver requested information to the consumer (after verification)
- The disclosure “shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request”
- Practical impact – consumer request that comes in on January 1, 2020 would require look-back to January 1, 2019

Employee/Prospective Employee Information (AB 25)

- Exempts the following information from the CCPA, except for the private right of action and notice requirement:
 - Personal information that is collected by a business about a natural person in the course of the person acting as a job applicant or employee (or owner, director, officer, medical staff member, or contractor) of that business, provided information is collected/used solely within the context of role as job applicant/employee
- Includes family information to extent collected/used to administer benefits or as emergency contact
- Businesses must still provide employees and job applicants CCPA-style notice
- Sunset provision – becomes inoperative on January 1, 2021

Business Contact Information (AB 1355)

- Limited carve out (from right to know, access, delete, opt-out of sale) for personal information collected/exchanged verbally or in writing between the business and the consumer, where:
 - consumer is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency; and
 - occurs solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency
- Sunset provision – becomes inoperative on January 1, 2021

Definition of “Sale”

- Broad definition of “sale” under CCPA
 - What is considered “valuable consideration”?
 - Who is a “third party”?
 - Definition of “third party” describes who is not a third party under CCPA
- A sale does not occur in certain circumstances, when:
 - Business is directed by the consumer to intentionally disclose PI or to interact with a third party (under certain conditions);
 - PI is shared with service providers, as that term is defined;
 - PI is transferred to a third party as part of a merger, acquisition, bankruptcy or certain other transaction
- To qualify as a service provider, there must be a written agreement between the parties with specific restrictions and requirements specified by the CCPA

Deep Dive – Can Data Be De-identified?

- “De-identified” information may not be covered by the CCPA, so businesses may wish to consider whether they can de-identify some of the personal data they collect
- CCPA (as amended) defines “de-identified” data to mean information that does not identify, or is not reasonably linkable to a particular consumer. Requires the business to:
 - Take reasonable measures to ensure the data is not re-identified
 - Make no attempt to re-identify the information
- What data could be subject to de-identification? Would de-identified data still be valuable or useful? Are there some data elements that cannot be de-identified consistent with other business goals?

Who is exempt and how is the CCPA enforced?
No Simple Answers

Are there any instances where the CCPA does not apply?

- Obligations of the CCPA do not restrict business's ability to:
 - Comply with federal, state, or local law
 - Comply with governmental inquiries, investigations, subpoenas
 - Cooperate with law enforcement agencies
 - Exercise or defend legal claims
 - Collect, use, retain, sell or disclose aggregated or de-identified information

Is Anyone Exempt From the CCPA?

- One entity-based exclusion. The CCPA does not apply to:
 - A provider of health care governed by Confidentiality of Medical Information Act or a covered entity under HIPAA, to the extent the provider / covered entity maintains patient information in the same manner as medical information or protected health information

Is Anyone Exempt From the CCPA?

- Other exclusions are information-based. The CCPA does not apply to:
 - Information collected, processed, sold or disclosed pursuant to the GLBA and implementing regulations
 - Information collected, processed, sold or disclosed pursuant to the Driver's Privacy Protection Act (DDPA)
 - The sale of PI to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report and use of information is limited by FCRA
- CCPA applies to information collected, processed, sold or disclosed outside of these statutes

GLBA Exemption

- GLBA covers nonpublic personal information (NPI) of consumers and customers of financial institutions
 - Customers and consumers are natural persons who establish a relationship with the financial institution (e.g., obtain financial product or service) or provide NPI to determine eligibility for financial product or service
 - NPI includes personally identifiable financial information (e.g., information provided to obtain financial product or service or resulting from transaction involving product or service or information obtained about consumer) and lists of persons that are derived from nonpublic information (e.g., customer lists)
- GLBA requires financial institutions to:
 - Provide initial and annual written notices summarizing information collection, use and dissemination practices
 - Provide customers with opportunity to opt out of having “nonpublic personal information” disclosed to unaffiliated third parties (except as otherwise permitted by exceptions)
 - Adopt policies and procedures to maintain security, confidentiality and integrity of customer records and data

GLBA Exemption

- CCPA exemption regarding the GLBA provides:
 - CCPA shall not apply to personal information collected, processed, sold or disclosed pursuant to the GLBA and implementing regulations
 - However, exemption does not apply to CCPA's private right of action for unauthorized access/data breaches
- Exemption is limited – applies only to information collected pursuant to the GLBA, which is a limited subset of information. Other information is still subject to CCPA

Service Providers

- Sharing information with a “service provider” is not a sale (i.e., consumer cannot opt-out)
- A service provider is an entity that “processes information on behalf of a business” for a business purposes pursuant to a written contract
- Written contract with service provider must include specific restrictions and requirements, including:
 - Deletion of data upon request
 - Prohibit the service provider from retaining, using or disclosing PI for any purposes other than for the specific purposes of performing service specified in the contract
 - Include a certification made by the SP that it understands and will comply with the restrictions
- Business is not liable if service provider violates restrictions, provided that the business does not have actual knowledge, or reason to believe, at the time of disclosure that the service provider intends to violate

Moving target

Further Changes on the Horizon

AG Regulations

- AG must “solicit broad public participation and adopt regulations” on or before July 1, 2020. Public hearings have occurred this year.
- AG regulations must address certain topics, including:
 - Update categories of PI and definition of unique identifiers to address “changes in technology, data collection practices, obstacles to implementation, and privacy concerns”
 - Establish any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights
 - Establish rules and procedures to “facilitate consumer’s ability to obtain information with goal of minimizing administrative burden on consumers, including rules on verifiable request”
- AG may not bring an enforcement action until 6 months after publication of final regulations or July 1, 2020, whichever is sooner

Multiple CCPA Amendments Passed

- A number of CCPA amendments passed in Sept. 2019 and are awaiting the Governor's signature
- Passed amendments were mostly clarifying in nature
- Some amendments are only applicable for a limited period of time (e.g., amendments regarding employee and business contact information)
- Many business-backed amendments failed
- Nonetheless significant pushback from privacy groups

New Proposed Ballot Initiative for 2020

- Alastair Mactaggart, who introduced the CCPA last year, has proposed a new ballot initiative for 2020 titled “The California Privacy Rights and Enforcement Act”
- “CCPA v2.0” would be even tougher on businesses that collect people’s PI. For example, the proposal would:
 - Create new rights around use and sale of sensitive PI (e.g., health information, precise geolocation information)
 - Provide extra requirements with respect to collection of PI from children under the age of 16
 - Require transparency around automated decision-making and profiling
 - Create a new agency in California (the California Privacy Protection Agency) to enforce privacy protections
- If ballot initiative passes, then it will be difficult to amend

State-Level Policy Also Continues to Evolve

- New consumer privacy law in Nevada
- A number of states have proposed comprehensive data-protection legislation (e.g., HI, IL, MD, MA, MS, NV, NJ, NM, NY, ND, PA, RI, WA)
- Some legislation mimic requirements of CCPA; others take different approach to data privacy
- Creates risk of patchwork of data-privacy requirements across states



Nevada's Consumer Privacy Law

- Nevada's SB 220 leapfrogged the implementation of the CCPA and became effective on October 1, 2019
- Covers "operators" who own or operate an Internet website or online service for commercial purposes and collect covered information from consumers who reside in Nevada and have a nexus with the state through transactions with state residents or other activities
- Each operator must establish a designated address for consumers to submit requests to opt out of certain sales, which is much more limited than CCPA

Getting prepared

Practical Steps Towards Compliance

CCPA Compliance Failures Could Be Costly

- California AG can seek statutory damages for violations of the CCPA that are not cured within 30 days
 - Up to \$7,500 per intentional violation, \$2,500 per unintentional violation
- Consumers whose “nonencrypted and nonredacted personal information... is subject to an unauthorized access and exfiltration, theft, or disclosure” (AB 1355) have limited private right of action against violators
 - Can recover between \$100 to \$750 per incident or actual damages, whichever is greater
 - Need not prove actual damages to qualify for statutory damages
 - May seek injunctive or declaratory relief
 - This right only attaches to compromise of data already protected under CA data breach notification statute
- Large-scale breaches that result in CCPA violations could thus impose significant penalties on organizations in addition to the standard expenses associated with breaches

Companies May Draw on GDPR-Compliance Work

- Even though coverage and requirements of GDPR and CCPA differ in many respects, they share many common types of obligations that organizations will need to address:
 - Identify necessary changes to address new individual rights
 - Update privacy notices and internal privacy policies
 - Review internal processes
 - Update recordkeeping
 - Update vendor agreements
 - Review security measures
 - Review data breach response plan

CCPA Readiness Steps

- **Perform Data Classification/Mapping for CCPA's Expanded Definition of Personal Information**
 - Survey systems and processes considering the CCPA's expanded definition of what is considered to be "personal information" to determine:
 - what information is collected,
 - how it is used, and
 - what may be subject to an exemption

CCPA Readiness Steps

- **Update Privacy Policies and Notices.**
- The CCPA requires:
 - Disclosure of the categories of personal information collected, sold, and disclosed for a business purpose in the last 12 months as well as information on how PI is used
 - Notice must be provided “at or before the point of collection”
 - Transparency regarding the rights conferred under it and a description of the methods for submitting a personal information or deletion request
 - A link to an opt-out page on the website

CCPA Readiness Steps

- **Determine whether you are selling (or disclosing “for monetary or other valuable consideration”) personal information, and, if so, build opt in/opt out functions and procedures**
 - The CCPA allows consumers to opt out of the sale of their personal information
 - Need to provide a function on website to allow for this and develop procedures for handling opt-out requests

CCPA Readiness Steps

- **Identify Service Providers and Update/Supplement Contracts**

- The CCPA allows businesses to share personal information with service providers (a defined term) without it being considered a sale (from which a consumer could opt out)
- To qualify as a service provider, the written agreement between the parties must contain certain provisions
- Analyze the data flow in their third-party relationships and amend written agreements accordingly

CCPA Readiness Steps

- **Evaluate Data Security/Review Incident Response Plan**
 - The CCPA includes a private right of action in the event of a data breach
 - Proposed amendments are likely to amend the private right of action
 - Revisit incident response plan to ensure it emphasizes rapid detection, containment and mitigation

CCPA Readiness Steps

- **Develop Policies and Procedures for Governance Program**
 - The new information rights will necessitate new, or changes to existing, internal privacy programs
 - Consider designating a role with responsibility for CCPA compliance and oversight
 - Have processes in place to receive and track consumer requests regarding personal information
 - Consider workforce training, particularly for workers that will be handling individual requests

Questions?