Coblentz
Patch Duffy
& Bass LLP

Spring / Summer 2023 Privacy Law Report

A Comprehensive Look at New Developments in Data Privacy Laws

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com

Spring / Summer 2023

Contents

Introduction

It has been a busy start to 2023 on the data privacy front: from new privacy laws being passed in several states and going into effect in others, to increases in privacy litigation and data breaches. Businesses need to be aware of new developments, new legal requirements, and steps that should be taken to comply with these laws and reduce business risk. This Overview highlights some of the most important privacy developments to be aware of for the coming year.

New State Privacy Laws

New comprehensive privacy laws in California and Virginia took effect on January 1, 2023, while new laws in Colorado and Connecticut are set to take effect on July 1. Other laws in Utah, Iowa, Indiana, Montana and Tennessee have passed, with many other states close to passing new laws and/or proposing and debating privacy legislation.

The recently passed state laws have many similarities, but differ on certain issues, creating compliance challenges for businesses operating in multiple states. For example, the majority of state laws apply only upon processing a certain volume of consumer data annually (typically, personal data of at least 100,000 consumers), but Utah requires both a processing minimum and an annual revenue threshold of $25M, while California law applies if either of those thresholds is satisfied. Additionally, while California allows individuals to limit the use of sensitive personal information in certain circumstances, several other states now require opt-in consent to process sensitive personal information. Certain states also require impact assessments or audits in connection with data processing that involves heightened risks of harm to consumers, including use of data for targeted advertising, profiling or other purposes. Notably, only California has included employees and job applicants within the definition of a “consumer.”

A brief overview of the state privacy laws in effect (or soon to be in effect as of July 1) is set forth below.

California - CPRA

The California Privacy Rights Act ("CPRA"), which was approved by California voters in November 2020 and went into effect on January 1, 2023, amends and expands on the California Consumer Privacy Act (“CCPA”) by giving consumers more control over their personal information. The CPRA applies to businesses that have $25M in annual global revenue, or process the personal information of 100,000 or more California consumers, or derive 50% of profits from selling or sharing personal information.

Some key changes in the CPRA include:

- Expanded scope of law to include employees, job applicants and B2B contacts as “consumers.”
- Expanded the definition of "personal information." The CPRA includes new defined categories of personal information such as sensitive personal information, which includes things like social security numbers, biometric information, precise geolocation data, race, ethnicity, and health information.
- Introduced the term “sharing” of personal information, meaning the disclosure of personal information for cross-context behavioral advertising purposes. Consumers now have the right to opt-out of sharing in addition to opting out of the selling of their personal information.
- Introduced the new consumer right to correct inaccurate personal information. Consumers can now request that businesses correct any inaccurate personal information they have collected.
- Created new data minimization, document retention, and data security requirements. Businesses must not collect more data, or retain it for longer, than needed.
- Introduced new contractual requirements for personal information disclosures to service

providers, contractors and third parties.
- Data protection impact assessments required for processing of sensitive data and processing that presents significant consumer risk, though regulations on these topics are forthcoming.
- Created the California Privacy Protection Agency, which will be responsible for enforcing privacy laws and imposing fines for violations.
- *Enforcement of the CPRA begins on July 1, 2023*.

Virginia - VCDPA

Like the CPRA, the Virginia Consumer Data Protection Act ("VCDPA") went into effect on January 1, 2023.

Key Provisions of the VCDPA:

- Applicability: The VCDPA applies to businesses that collect or process the personal data of at least 100,000 Virginia residents or derive at least 50% of their revenue from the sale of personal data and process the personal data of at least 25,000 Virginia residents.
- Consumer Rights: The VCDPA gives Virginia residents the right to access, correct, and delete their personal data, as well as the right to opt-out of the sale of their personal data and the right to object to the processing of their personal data for certain purposes. Businesses are also required to obtain explicit opt-in consent from consumers before collecting sensitive personal data.
- Data protection impact assessments required for processing sensitive data, profiling (under certain circumstances), selling and using data for targeted advertising, and processing that presents a heightened risk of harm.
- Enforcement: No private rights of action. The VCDPA grants the Virginia Attorney General the authority to enforce the law, and it also provides a private right of action for consumers to seek damages for violations of their rights under the law.

Colorado - CPA

The Colorado Privacy Act ("CPA") goes into effect on July 1, 2023.

Key Provisions of the CPA:

- Applicability: The CPA applies to companies that conduct business in Colorado or produce products or services that are intentionally targeted to Colorado residents and that either control or process the personal data of 100,000 or more consumers, or derive revenue or receive discounts from the sale of personal data and control or process the personal data of at least 25,000 consumers.
- Consumer Rights: The CPA gives Colorado residents the right to access, correct, delete, and obtain a copy of their personal data that has been collected by businesses. Consumers also have the right to opt-out of the sale of their personal data and to request that their personal data not be processed for certain purposes. Businesses are also required to obtain explicit consent from consumers before collecting sensitive personal data.
- Data protection impact assessments required for processing that presents a heightened risk of harm to consumers i.e., processing sensitive data, processing personal data for purposes of targeted advertising or for profiling (under certain circumstances), and selling data.
- Enforcement: No private right of action. The CPA grants the Colorado Attorney General the authority to enforce the law, and it also provides a private right of action for consumers to seek damages for violations of their rights under the CPA.

Connecticut - CTDPA

The Connecticut Data Privacy Act ("CTDPA") goes into effect on July 1, 2023.

Key Provisions of the CTDPA:

- Applicability: The CTDPA applies to businesses that collect or process the personal data of at least 100,000 Connecticut residents or derive at least 50% of their revenue from the sale of personal data and process the personal data of at least 25,000 Connecticut residents.
- Consumer Rights: The CTDPA gives residents the right to access, correct, and delete their personal data, as well as the right to opt-out of the sale of their personal data. Businesses are also required to obtain explicit consent from consumers before collecting sensitive personal data.
- Data protection impact assessments required for processing that presents a heightened risk of harm to consumers i.e., processing sensitive data, processing personal data for purposes of targeted advertising or for profiling (under certain circumstances), and selling data.
- Enforcement: The CTDPA grants the Connecticut Attorney General the authority to enforce the law, and it also provides a private right of action for consumers to seek damages for violations of their rights under the law. No private right of action.

Other State Privacy Laws

In addition to the laws above, Utah, Iowa, Indiana, Montana, and Tennessee have passed comprehensive data privacy laws, with Texas and other states close to doing so. Many other states have proposed legislation and are proceeding with privacy laws, with more states sure to follow in the coming months. The newly passed and proposed laws are largely modeled on the state laws above, but certain differences in each state law will continue to provide compliance headaches for companies doing business nationwide. Companies should continue to monitor these developments in states where they conduct business.

California's Upcoming Age-Appropriate Design Code Act

California's new Age-Appropriate Design Code Act ("CAADCA"), goes into effect on July 1, 2024. The new law promulgates privacy, data, and safety protections for children and teens using online platforms. Businesses subject to the CPRA should review the requirements of CAADCA closely to determine what data protection measures should be updated as the new law expands upon existing laws geared towards minors, such as California's Parent's Accountability and Child Protection Act and the federal Children's Online Privacy Protection Act ("COPPA").[1]

Businesses Subject to CAADCA

CAADCA applies to businesses as they are defined under the CPRA.[2] Specifically, CAADCA applies to businesses that provide online services, products, or features that are "likely to be accessed by children" who are under age 18. An online service, product, or feature is "likely to be accessed by children" based on certain factors, including whether it is directed to children, routinely accessed by a significant number of children, has advertisements marketed to children, has design elements that are known to be of interest to children (i.e., games, cartoons, music, and celebrities who appeal to children), and has a significant audience that is determined to be children.

Overview of CAADCA Requirements and Restrictions

CAADCA requires covered businesses to implement the following affirmative actions:

- Create a Data Protection Impact Assessment ("DPIA") that includes detailed information about their online service, product, or feature that is "likely to be accessed by children."
- Configure all default privacy settings offered by the online service, product, or feature to offer a high level of privacy.
- Provide privacy information, terms of service, policies, and community standards using clear language suited to the age of the children. Provide prominent, accessible, and responsive tools to help children or parents or guardians exercise their privacy rights and report concerns.
- Provide an obvious signal to a child when the child is being monitored or tracked by the online service, product, or feature.

1 For instance, CAADCA is broader than the COPPA, which is limited to operators of websites or online services directed to children under age 13.

2 The CPRA defines a "business" as any for-profit entity operating in California that collects personal information of California residents and satisfies one of three requirements: (i) the company has annual gross revenues of more than $25 million; (ii) the company buys, sells, or shares personal information of at least 100,000 California residents; or (iii) the company derives at least 50% of its annual revenues from selling or sharing California residents' personal information.

CAADCA also prohibits covered businesses from engaging in the following actions:

- Using a child's personal information in a way that is, "materially detrimental to the physical health, mental health, or well-being of a child."
- Collecting, selling, sharing, or retaining the personal information of children for any reason other than a reason for which the personal information was collected, unless the business can demonstrate a compelling reason that aligns with the best interests of children.
- Using dark patterns, which are online experiences designed to encourage children to provide too much personal information.
- Profiling children, though this prohibition is subject to certain exceptions.
- Using personal information to estimate the age of a child for any other purpose than estimating age, or retaining that personal information longer than necessary to estimate age.

Enforcement of CAADCA

CAADCA authorizes the Attorney General to seek an injunction or civil penalty against any business that violates its provisions. The Attorney General can hold violators liable for a civil penalty of up to $7,500 per affected child. The new law gives companies an opportunity to cure any alleged violation within 90 days so that they can avoid these penalties.

Comprehensive Federal Privacy Law?

Comprehensive federal privacy legislation has been proposed but remains under debate, and there is no telling when or in what form it might ultimately be passed. Last year, Congress advanced the American Data Privacy and Protection Act ("ADPPA") out of committee, but it was met with opposition on the House floor. In March 2023, the House Committee on Energy and Commerce held multiple hearings in advance of releasing a new draft of the ADPPA, which is expected to be released imminently and include significant changes.

The ADPPA, if passed, would create national standards and safeguards for personal information collected by companies. The ADPPA would apply to any entity that collects, processes, or transfers covered data and is subject to the jurisdiction of the Federal Trade Commission, including nonprofits, telecommunication carriers, and other companies. In its earlier form, the ADPPA established the right to access, correct and delete personal data, required companies to provide consumers a means to opt-out of targeted advertising, provided additional protections for individuals under the age of 17, and prohibited the use of personal data to discriminate based on protected characteristics. The ADPPA would also impose certain requirements on service providers and third-party entities.

One of the important issues for debate is whether and to what extent a federal privacy law would preempt the data privacy laws passed by individual states.

While many businesses are pleading for a uniform federal privacy standard, there is substantial opposition to a federal law that would entirely preempt the strong data privacy laws that have been enacted by the states, especially the CPRA, which created its own robust enforcement regime and privacy protection agency. If passed, the ADPPA would override state data privacy laws and prevent states from acting in areas where they have experienced recent progress. Progressive states, like California, that have more stringent privacy protections view the ADPPA as weakening their consumer privacy protections.

On the other hand, covered entities, particularly small business owners, are currently burdened by a complex patchwork of legal obligations that vary from state-to-state. Passage of a comprehensive federal standard such as the ADPPA would allow companies to more easily comply with requirements for data privacy protection. For those states that have been unable to successfully pass data privacy laws, the ADPPA would mark a significant step towards offering nationwide data privacy protection across all states.

Overall, some kind of a federal privacy law appears likely, but the timing and scope of such a law remains unclear. In the meantime, businesses are obligated to comply with state laws in the jurisdictions where they operate.

EU-US Privacy Framework Status

It has been nearly three years since the Court of Justice of the EU ("CJEU") invalided the EU-US Privacy Shield in its Schrems II decision on July 16, 2020. At that time, the CJEU determined that because the requirements of US national security, public interest, and law enforcement have "primacy" over the data protection principles of the EU-US Privacy Shield, the data transferred under Privacy Shield would not be subject to the same level of protections prescribed by the GDPR.

Since then, companies that exchange or transfer data between the EU and the US have faced a great deal of legal uncertainty and burdensome procedures (such as Standard Contractual Clauses) in attempting to execute compliant cross-border data transfers.

On October 7, 2022, as a replacement for the EU-US Privacy Shield, and in an attempt to lay the groundwork for an EU adequacy decision that would facilitiate seamless EU-US data transfers, President Biden signed an Executive Order directing steps that the US will need to take to implement its commitments under the new EU-US Data Privacy Framework.

The Executive Order provides that US signals intelligence activities shall be "necessary" and "proportionate" to a "validated intelligence priority." Each sector of the US intelligence community that handles personal information collected through signals intelligence must establish policies and procedures to minimize the dissemination and retention of personal information. Each sector must also maintain appropriate training requirements to ensure that employees with access to signal intelligence know and understand the requirements of the Executive Order.

The Executive Order requires the Attorney General, in consultation with the Secretary of Commerce, the Director of National Intelligence, and the Privacy and Civil Liberties Oversight Board, to appoint judges to serve on a newly created Data Protection Review Court.

The Executive Order also requires intelligence agencies to adjust their policies consistent with Executive Order within one year, by October 7, 2023. US organizations will need to certify under the new EU-US Data Privacy Framework, which will require committing to comply with a detailed set of privacy obligations.

In December 2022, the European Commission published a Draft Adequacy Decision meant to replace the Privacy Shield. However, on February 14, 2023, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs published a draft resolution urging the European Commission not to adopt the Adequacy Decision until certain further reforms in US law have been made. On February 28, 2023, the European Data Protection Board ("EDPB") issued an opinion on the Draft Adequacy Decision welcoming substantial improvements on the EU-US Data Privacy Framework, but expressing concerns and requesting clarifications on various points. On May 11, 2023, the European Parliament voted on a resolution calling for the European Commission not to adopt an Adequacy Decision until the recommendations made in the European Parliament's resolution and the EDPB opinion are fully implemented. In sum, a solution to the current challenges of the EU-US data transfers may not be imminent. Until a new adequacy decision is announced, companies must continue operating under the current structure, including using the new Standard Contractual Clauses.

Trends in Privacy Litigation and Enforcement

Privacy-related litigation continues to be on the rise, with many lawsuits being filed under the California Invasion of Privacy Act ("CIPA") and the Video Privacy Protection Act ("VPPA"), among other laws, focusing on how personal information is collected, used, and disclosed on business websites. CIPA claims have focused on session recording technologies and chatbot functions, typically operated by third parties on business websites. The claims typically allege that the third party vendor providing the session recording or chat technology is “eavesdropping” on and therefore “wiretapping” the communication between the consumer and the business and collecting personal information in connection with session recording or chat functions. Although courts have come to different conclusions on the merits of these cases, recent decisions have moved towards dismissing CIPA wiretapping claims where the third party vendor is only collecting and processing information on behalf of the business, as opposed to using or selling the personal information for marketing or targeted advertising. Businesses should continue to monitor cases and decisions in this area.

The VPPA, a 1988 law focused on privacy of video store rental histories, has been another popular basis for recent litigation, with many complaints being filed against businesses that stream videos on their website and then disclose, through analytics or otherwise, identifying personal information and content of videos viewed to third parties. Although courts are still grappling with how to deal with the application of this law to new technologies, with potential damages of at least $2,500 per affected consumer, violations can be devastating, and defending against such lawsuits – even when they lack merit – can be very costly for companies.

Businesses can reduce the risk of such suits by understanding how their websites are using tracking analytics and pixels, including Meta Pixel, Google Analytics, and other software technologies monitoring website interactions and activities by consumers. Businesses should consider implementing proper notification requirements and opt-in or opt-out mechanisms for consent before using such technologies or otherwise disclosing personal information from consumer website interactions to third parties.

On the enforcement front, the big news was last year’s first CCPA enforcement action by the California Attorney General against Sephora USA, Inc., which resulted in a settlement payment by Sephora of $1.2 million and injunctive terms. This was the first settlement under the CCPA, and arose from Sephora’s practices of selling consumer data through third-party tracking technologies on its website and mobile apps while stating in its privacy policy that it was not selling data and refusing to honor opt-out signals from internet browsers. As a result, all companies are encouraged to review the use of third party analytics and tracking technologies to ensure that their disclosure, particularly any sales, of consumer data is consistent with their privacy policy and permitted by applicable laws.

Things are certain to get more exciting starting July 1 when formal enforcement of the CPRA begins. It will be interesting to see how the new California Privacy Protection Agency prioritizes privacy enforcement and what having a dedicated privacy enforcement agency will look like going forward.

Health Privacy

HIPAA Tracking Technologies

On December 1, 2022, the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") issued guidance to covered entities and their business associates ("regulated entities") concerning online tracking technology and the collection and transmission of protected health information ("PHI") that may implicate the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Healthcare entities often use tracking technologies such as cookies, pixels, and web beacons. In response to a wave of lawsuits filed regarding disclosure of patient information through such tools, OCR issued guidance stating that such tools' collection of information may implicate HIPAA, including with respect to healthcare entities' appointment scheduling pages, patient portals, and mobile applications. In sum, the OCR guidance states that regulated entities, "are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

The OCR Guidance appears to take a broad view of information that constitutes PHI and that can be swept into online tracking technologies, and lawsuits have already been filed in 2023 alleging violations and citing to the OCR Guidance.

This is a good time for regulated entities to review their use of tracking technologies in light of the OCR Guidance, and in particular to ensure that they have Business Associate Agreements in place with vendors that provide tracking technology.

Biometric Privacy Laws

Biometric technology, which uses unique physical or behavioral characteristics such as fingerprints, facial recognition, and iris scans for identification and authentication, has become increasingly popular in various industries. However, as the use of biometric data raises privacy concerns, several states along with some metropolitan cities in the US have enacted or proposed biometric laws to regulate the collection, use, and storage of such data.

Currently, there are three states with laws specifically focused on biometric collections. Illinois was the first state to enact a biometric privacy law, the Biometric Information Privacy Act ("BIPA"). BIPA requires companies to obtain written consent from individuals, including employees, before collecting their biometric data, inform individuals about the purpose and duration of data collection, and provide written release before sharing the data with third parties. BIPA also imposes strict requirements for the storage and destruction of biometric data, and allows individuals to sue companies for statutory damages in case of violations.

Washington also regulates the collection of biometric data from businesses. Under Revised Code of Washington, Title 19, Chapter 19.375, "[a] person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial use." RCW 19.375.020(1). Similarly, Texas prohibits businesses from, "captur[ing] a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier." Tex. Bus. & Comm. Code, Title 11, Subt. A, Chapter 503, § 503.001(b).

Additionally, some cities have enacted ordinances that also regulate the collection of biometric information – including the use of facial recognition tools of customers and employees on the premises. Under Chapter 12 in the New York City Administrative Code, "[a]ny commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language . . . that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable." N.Y.C. Admin. Code § 22-1202(a). Portland, Oregon similarly bans the use of facial recognition technology by businesses. Under Chapter 34.10 of the Portland City Code, unless facial recognition is used for user verification purposes for employment purposes, "a Private Entity shall not use Face Recognition Technologies in Places of Public Accommodation within the boundaries of the City of Portland." Portland City Code §§ 34.10.030, 34.10.040. "Places of Public Accommodation" include "[a]ny place or service offering to the public accommodations, advantages, facilities, or privileges whether in the nature of goods, services, lodgings, amusements, transportation or otherwise." Id. at

§ 34.10.020(D)(1). Many of these biometric laws allow for private rights of actions that can result in hefty fines. For example, earlier in the year, a class-action lawsuit was brought against Amazon alleging Amazon's cashierless stores violated New York City's biometric laws. Businesses should be cognizant and review their biometric collection practices. These biometric laws generally require some sort of affirmative notice at the point of collection and consent from the individual.

Beyond these biometric-specific laws, many states (California, Virginia, Colorado, and Connecticut, with more on the way), have recently passed comprehensive data privacy statutes that also regulate the collection, use, and disclosure of biometric information of consumers (and, in California, employees). Companies should carefully review their collection of biometric information and assess compliance with applicable laws.

SEC Cybersecurity Rule

As cyber threats continue to evolve and pose significant risks to businesses, the Securities and Exchange Commission (“SEC”) has made clear – through proposed rules related to cybersecurity, enforcement actions, public statements, and an enhanced "Crypto Assets and Cyber Unit" within the Division of Enforcement – that it expects public companies and registered entities to promptly assess the materiality of cybersecurity incidents and make swift discolsures of material incidents. In 2022 and 2023, the SEC has proposed cybersecurity rules aimed at strengthening the cybersecurity posture of companies operating in the United States. With the increasing reliance on technology and the growing frequency and sophistication of cyberattacks, cybersecurity has become a top concern for companies across all industries. The SEC recognizes the need to safeguard the integrity and stability of the capital markets, and has been actively working to address cybersecurity risks.

The proposed rules are designed to enhance the protection of sensitive information and systems, and promote the resilience of companies against cyber threats. They entail expansive requirements that, if adopted, public companies will need to comply with to ensure their cybersecurity practices are in compliance. The key obligations for businesses are as follows:

- Report any cybersecurity event within four business days of determining that it was a material incident.
- Report material incidents that, in conjunction with other incidents, become material "in the aggregate."
- Mandatory disclosures regarding the board of directors' oversight of cybersecurity risk as well as details about the cybersecurity expertise and experience of individual board members.
- Share updates on previous incidents in regular SEC disclosures.
- Adopt and implement written cybersecurity policies and procedures.
- Conduct regular risk assessments to identify and assess cybersecurity risks and vulnerabilities.
- Establish and implement an incident response plan that outlines the procedures to be followed in the event of a cybersecurity incident.
- Maintain records of cybersecurity policies, procedures, risk assessments, incident response activities, and other cybersecurity-related matters for a period of at least five years.

The proposed SEC cybersecurity rules go beyond what is excerpted above and will have significant implications for companies operating in the US when implemented. Final rules are expected to be issued soon. Getting a head start on compliant procedures and practices will help companies avoid potential penalities and reputational damage down the line.

Data Breach Response

2023 has already seen several major data breaches, and we can expect the increase in data breaches along with resulting litigation to continue. In particular, AI and machine learning developments are rapidly changing the cybersecurity landscape in both positive and negative ways. While powerful AI and machine learning tools are being developed to aid in cyber-defense, they can also be used by hackers and threat actors to identify and target vulnerabilities.

With data breaches, it is not a matter of "if" but "when." Companies should ensure preparedness with data breach response plans, including identifying the team of in-house and external resources that will be available and prepared to put the plan into action as soon as a security incident or data breach arises.

Some key components of a data breach response action plan include:

- Create an Incident Response Plan, including a detailed a roadmap to the systems that could be affected, a detailed outline of the steps to be taken, and a list of who to call during and after the incident, and all consumer and regulatory notices that may be required – and keep a printed copy in case you are unable to access your electronic copy during an incident.
- Identify your internal incident response team, including who will be responsible for decision-making during the incident.
- Obtain cyber insurance and/or review your current policy to confirm scope and coverage for cyber incidents.
- Identify and engage your external incident response team so that it is positioned to activate promptly when a security incident or data breach occurs, including outside counsel, data forensics investigators, and an external communications firm.
- Practice and discuss your incident response plan regularly, including through tabletop trainings with your team.
- Review your Incident Response Plan regularly to ensure it is up to date.

Contact

If your company needs assistance with any privacy issues, the Coblentz Data Privacy and Cybersecurity attorneys can help. Please contact a member of the Data Privacy and Cybersecurity team for further information or assistance.

Authors

Scott C. Hall

Head of Data Privacy and Cybersecurity Group
Partner
San Francisco

Contact
415.772.5798
shall@coblentzlaw.com

Mari S. Clifford

Associate
San Francisco

Contact
415.268.0504
mclifford@coblentzlaw.com

Sabrina A. Larson

Partner
San Francisco

Contact
415.268.0559
slarson@coblentzlaw.com

Amber Leong

Associate
San Francisco

Contact
415.268.0535
aleong@coblentzlaw.com

Bina Patel

Associate
San Francisco

Contact
415.268.0563
bpatel@coblentzlaw.com

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com