# Contact Center Compliance Under the Biden Administration

On January 20, 2021 Joseph Biden was sworn in as the 46th president of the United States. Presidential elections are held every 4 years. Joseph Biden is a Democrat. The prior incumbent, Donald J Trump, was a Republican. In developing policy Republicans broadly accept the notion that a capitalistic economy functions best in an environment of limited regulation. President Biden and Democrats have a more sympathetic view of regulations. Biden is characterized as an "Old School" democrat. He is a strong supporter of labor rights and federal regulations that protect consumers and tend to even the playing field for large and small businesses.

This paper proposes what the contact center regulatory environment will become under the new administration. Ongoing events such as the coronavirus, economic conditions, politics, and events not yet even anticipated can alter these projections. That said, we can make some very meaningful forecasts of the regulatory environment by examining cabinet level appointments, executive orders, legislative initiatives, and public statements and reports.

**It is our belief, based on the above is sources, the Biden administration will:**

1. Develop a national policy and enact legislation confers certain privacy rights to all US citizens. This will be modeled after the European GDPR and privacy laws enacted by US states.
2. Continue to ease financial hardships imposed by the Covid crisis through the extension and enhancement of prior legislation.
3. Expand monitoring and enforcement of the laws and regulations administered by the Consumer Financial Protection Bureau (CFPB).
4. In general, pursue policies and legislation that seeks to unify under a federal umbrella current state rules such as privacy protection, data security, and fraud prevention.

 

PELORUS associates

It will take a year or two to assess actual convictions and penalties. However, to get an idea of what the pace would be like under an aggressive pro-consumer administration we can draw some inferences from legal actions triggered by the California Consumer Protection Act. While enforcement of the CCPA only began July 1, 2020 sixteen cases have already been filed, primarily claims against unauthorized release of Personally Identifiable Information (PII). Familiar names identified as defendants include Google, Salesforce.com, Zoom Video Communications, Shutterfly, and Marriott international.

We will close this paper with a summary of actions contact centers should consider in anticipation of a new highly aggressive approach to regulation.

# Appointments

The president has the power to appoint hundreds of positions in the federal bureaucracy. Two government agencies particularly important to the customer care industry are the Federal Trade Commission and the Consumer Financial Protection Bureau.

### Federal Trade Commission (FTC)

President Biden has appointed Rebecca Kelly Slaughter as Acting Chairwoman of the FTC. She is known for her views on modernizing and strengthening antitrust laws to better protect the public and U.S. markets from rising monopoly power and anticompetitive mergers and conduct. Lina Khan is picked to become a commissioner at the Federal Trade Commission. At age 32, she is the youngest person to hold this position. A noted tech critic, Khan would get to vote on important cases involving antitrust and consumer protection at the FTC. That could include a decision on whether to bring an antitrust lawsuit against Amazon, which it has reportedly been investigating, as well as whether to block acquisitions by large companies.

### Consumer Financial Protection Bureau (CFPB)

President Biden has nominated current FCC Commissioner Rohit Chopra as director of the powerful Consumer Financial Protection Bureau. The CFPB oversees a $600 million budget and a 1,600-member workforce dedicated to protecting consumers from unfair, deceptive, and abusive practices through the enforcement of federal consumer financial law. During his confirmation hearing Chopra pledged to retain the Covid-inspired forbearance policies in place to keep lenders from foreclosing on homeowners.

"We must not forget that the financial lives of millions of Americans lay in ruin," he said. "Many have seen their jobs disappear and will not be able to easily resume their [rent and mortgage] payments."

Under the Obama presidency supervision and enforcement was very aggressive. The CFPB

 

collected $12 billion in fines for consumer abuses during the tenure of Richard Cordray, the Bureau's inaugural Director. However, the Trump administration regulations and enforcement was largely ineffectual. President Biden has said his tenure is not a third Obama term. He plans to move the administration from Trump's "principles-based" approach to a "rules-based" environment.

Based on the administration's public statements and personnel appointments we can reasonably assume that enforcement will be much more rigorous than under the Trump administration.

## Consumer privacy rights

The United States is unique among industrialized nations in that it does not have a national law assuring consumer privacy rights. Attempts have been made. The Obama administration drafted the Consumer Privacy Bill of Rights Act of 2015. This included key protections such as those included in the European General Data Protection Regulation (GDPR). Opposed by special interests and incompatible with priorities during the Donald Trump era, the bill languished. However, with the election of Joe Biden who is a strong advocate for consumer privacy rights and with slim majorities in the US House of Representatives and Senate, we can reasonably anticipate the passage of the nation's first comprehensive privacy bill at some point during the Biden presidency. A federal privacy statute enjoys broad public support and there is also growing pressure from international enterprises and governments for a single uniform set of requirements rather than the patchwork of state bills that are now working their way through state legislatures.

### Consumer Online Privacy Act (COPRA)

At this time, the Consumer Online Privacy Act is the only federal privacy bill working its way through Congress.

The purposes of COPRA are to:

- Provide consumers with foundational data privacy rights,
- Create strong oversight mechanisms, and
- Establish meaningful enforcement.

Protections applied to "covered data." Covered data is defined as anything that is "linked or reasonably linkable to an individual or a consumer device, including derived data." This could include biometric information, geolocation data, and online activities. Presumably, recorded voice and data interactions would be included if it can be tied to a specific individual.

 

The law applies to “covered entities.” These are organizations that process or transfer consumer data.

Covered entities are required to -

- Make their privacy policy publicly available and provide individuals access to their personal data.
- Delete or correct, upon request, information in an individual's data.
- Export, upon request, an individual's data in a human-readable and machine-readable format.
- Establish data security practices to protect the confidentiality and accessibility of consumer data.
- Designate a privacy officer and a data security officer to implement and conduct privacy and data security programs and risk assessments.

Covered entities must not -

Engage in deceptive or harmful data practices.

- Transfer an individual's data to a third party if the individual objects.
- Process or transfer data beyond what is reasonably necessary or for which they have obtained affirmative express consent.
- Process or transfer data on the basis of specified protected characteristics (e.g., race, religion, or gender.)
- Condition the provision of a service or product on an individual's agreement to waive their privacy rights.

In a civil action which the plaintiff prevails penalties are (a) an amount not less than $100 and not greater than $1000 per violation per day or actual damages, whichever is greater (b) punitive damages, (c) reasonable attorney’s fees and litigation costs, and (d) any other relief that the court determines appropriate.

### The California Consumer Privacy Act (CCPA)

The CCPA went into effect January 1, 2020 with the goal of protecting and regulating collection and sharing of “personal information.” It is aimed specifically at for-profit entities that collect or receive personal information from California residents, and meets one or more of the following criteria

- Has annual gross revenue that exceeds US $25 Million, annually

 

- Receives, buys, or sells shares, directly or indirectly, the personal information of 50,000 or more California residents, or
- 50% or more of its annual revenue is derived from the sale of personal information about California consumers.

Provisions particularly applicable to contact centers include

- Consumers have the right to request that a business that collects personal information disclose to that consumer the categories of personal information collected, the categories of sources from which that information was collected and the business or commercial purpose for collecting or reselling the information.
- Consumers may request that a business that collects personal information delete that personal information and the business must generally comply, unless the information is essential for conducting business with the customer.
- A business that sells personal information to third parties must notify consumers that the information may be sold, and the consumer has the right to opt out of the sale.
- If there is a security breach of computerized consumer records containing personal data, the organization must notify each individual to whom it maintained information. It does not matter if the data is maintained in or outside of California
- Civil penalties shall not be more than $2500 per violation or $7500 per each intentional violation. There is no maximum for multiple violations. All proceeds from violations will be deposited in the Consumer Privacy Fund

On March 2, 2021 Virginia enacted the Consumer Data Protection Act becoming the second state to legislate privacy rights.

### Electronic Communications Privacy Act

Workplace monitoring of employee communications is common in many industries and almost universal in contact center environments where quality monitoring is considered essential to achieving targeted levels of customer care.

The Electronic Communications Privacy Act (ECPA) was enacted to create promote " the privacy expectations of citizens and the legitimate needs of law enforcement." Congress also sought to support the creation of new technologies by assuring consumers that their personal information would remain safe. According to the Electronic Privacy Information Center, “In general, the statute bars wiretapping and electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, and the use or disclosure of information unlawfully obtained through wiretapping or electronic eavesdropping.” The ECPA contains several

 

exceptions of particular importance to employers. The first is the business purpose exception which permits employers to monitor oral or electronic communications as long as a company can show a legitimate business purpose for doing so. The second is the consent exception which allows employers to monitor employee communications provided that they have the employees consent.

Individuals who violate ECPA face up to five years in prison and fines up to $250,000. Victims are also entitled to bring civil suits and recover actual damages, in addition to punitive damages and attorney's fees.

## Consumer Protections

The Consumer Financial Protection Bureau enforces over a dozen consumer financial protection laws, including the Fair Credit Reporting Act , Fair Debt Collection Practices Act, and Truth-in-Lending Act. Under the Obama presidency supervision and enforcement was very aggressive, then lagged during the Trump administration. President Biden has voiced his support for consumer protections and appointed key people to support a return to the Obama era of regulation and enforcement.

Current priorities of the Consumer Financial Protection Bureau include

- Supporting efforts to reform the payday lending industry
- Increasing enforcement activity in the student lending space
- Re-examining bank overdraft charges
- Enforcing provisions of the federal CARES Act and American Rescue Act that extended temporary relief from mortgage payments backed by the Federal Housing Administration and rent for properties financed by federally insured agencies.
- Ensuring more equitable approval of personal and mortgage loans. President Biden himself has proposed the creation of a public credit reporting agency within the CFPB to compete with the three credit bureaus.
- Create an unfair or deceptive acts or practices framework for preventing and remedying discrimination in lending practices.

On January 5, 2021, the CFPB's Taskforce on Federal Consumer Financial Law released a report with suggestions on how to improve consumer protection in the financial marketplace. The Report makes 100 recommendations to the CFPB, Congress, and state and federal regulators.

 

An important distinction between the way consumer finance laws were enforced under the Trump and now the Biden administration is stronger focusing on individuals for culpability rather than the business entity itself. This is in response to criticism that business leaders in the past have not sufficiently experienced consequences for the actions of their companies.

## Preparations you can take

Many of the anticipated privacy protection and disclosure rules discussed in this white paper are already in place, albeit on a sector specific basis. Examples include the European General Data Protection Regulation, Health Insurance Portability and Accountability Act, Fair Debt Collections Practices Act, Truth in Lending Act, and Telemarketing Sales Rule.

### Suggested practices

- Include compliance in agent training programs
- Include compliance in quality monitoring evaluations
- Secure written or oral agreements from agents confirming their willingness to be recorded in the course of their work.
- Discourage agents from requesting personally identifiable information during the course of conversation unless you have the caller's authorization on file, or the information is essential to the conduct of the business.
- Make it a practice to extend recording to departments and individuals beyond the contact center to customarily interact directly with consumers regarding matters that could impact privacy. Examples include loan officers, collectors, inside sales personnel, and human resources departments.
- If other parties will have access to the recorded voice or data interaction it would be prudent to forewarn them in the recorded greeting. For example, Microsoft Office includes the following in their greeting Thank you for choosing office 365. To help us improve the quality of our products and services and training this call may be recorded or monitored and information collected on this call may be transferred to other countries.
- Be prepared to retrieve and provide upon legitimate request specific recorded interactions.
- Maintain strict controls over who has access to encrypted interactions which may include personally identifiable information (PII).
- Coordinate closely with the individual or team tasked with compliance in your organization.

 

## Suggested technology investments

- Contact volume has skyrocketed during the pandemic and will probably continue on a higher-than-normal level as people switch to online products and services. Your technology must be scalable to seamlessly respond to varying levels of demand and to be able to make on the fly software changes as rules and regulations change. The cloud model offers the scalability, flexibility, and responsiveness you need in the current and future environment.
- The remote worker model is here to stay. This is another persuasive reasons why the cloud architecture is best suited to today's contact center model.
- The vendor of your recording solution and related applications should follow the precepts of "Compliance by Design" which enables rapid response to changing laws and regulations.
- The contact center recording and quality monitoring apparatus should be able to detect possible violations during the course of an interaction. A superior solution will trigger alerts to agents if they need to provide disclosures or if there is risk of securing private information without the consent of the customer.
- Best in class recording solutions will include a dashboard from which management can monitor system performance and agent compliance.
- The recording system must be able to record and reconstruct omnichannel interactions, including audiovisual conferences.
- At the risk of losing card acceptance privileges, organizations must deploy technology that meets the security standards established by the Payment Card Industry. The standards continue to evolve. Among other things, multifactor authentication and encryption are requirements. Your recording system should be PCI – DSS compliant with all applicable requirements and engineered to rapidly adapt to change.
- Recording and analytics should go hand-in-hand. AI infused analytics should be able to detect patterns and possible causes for compliance exposures.

Compliance is nothing new for contact centers, but years of lax enforcement has restrained the urgency and priority of understanding the many requirements and developing and implementing action plans to assure compliance.

 

## About the author

**Dick Bucci** is Founder and Principal of Pelorus Associates where he specializes in contact center technologies and compliance. Dick has authored 19 in-depth market research reports on workforce optimization applications and numerous articles and white papers. Prior to founding Pelorus Associates he was a senior sales and marketing executive with leading telecommunications manufacturers.