Legal and Regulatory Outlook for Workforce Engagement - *Will You Be Ready?*

Author: Dick Bucci, Principal, Pelorus Associates

These past two years have been extremely impactful on the legal and regulatory front. The two most notable events include the implementation of the European Union's General Data Protection Act and the California Consumer Privacy Act, which went into effect June 20, 2021. There are many other international, federal, state, and local laws and regulations that were passed or went into effect during these past two years and the number of initiatives appears to be increasing. Legislators at all levels are feeling pressure from voters to protect individual privacy and help prevent the major security lapses that have proved costly to consumers and to corporate reputations.

While compliance may not always be top of mind in busy contact centers, you can be sure that compliance is very important to the senior executives that are responsible for the overall company success. While the cost of compliance varies depending on who does the number crunching, *Investor's Business Daily* reports that the cost of regulations to the U.S. economy is huge — roughly $2 trillion a year or about 12% of our entire economy. CNBC reported that firms may have to pay up to $55 billion in initial compliance costs as a result of the California Consumer Privacy Act.

In this brief report we will explore the forces behind regulatory change and point to what we believe are specific rules and regulations that may directly impact the contact center. We will close with some helpful recommendations about investments and practices that will help contact center managers avoid potential costly violation lapses. The reader should understand that the contents of this paper should not be interpreted as legal advice.

What's Behind the Trend?

There is little doubt that the pace of new regulations and regulatory rulings is continuing to increase in the United States. There are many factors that account for this increasing pace of regulatory change. A few of the principal forces we can point to are:

- *Outrage over privacy infringements:* The number of data breaches in the U.S. has skyrocketed within the past decade from 662 in 2010 to over a thousand by 2020. The most notorious of these was the 2013 incursion of online platform Yahoo where hackers stole user information associated with at least 1 billion accounts in 2013. Privacy breaches, particularly of financial information, hit consumers in the wallet. While the average loss is not large, users can spend many hours trying to clean up problems after the breach.
- *More consumer-friendly administration:* Joe Biden was sworn into office on January 21, 2021. President Biden is a friend of labor and the consumer. Through his appointments and his public statements, he has indicated a drive to strengthen consumer privacy rights and improve wages, benefits, and working conditions for employees.
- *Growth of the contingent workforce:* One of the many long-term impacts of the COVID-19 pandemic is a sea change in the way work is administered and managed. According to the American Time Use Survey as reported by Newsweek, the portion of people in the U.S. working from home grew from 22% to 42% between 2019 and 2020. The proportion of men working remotely rose by 16%, while the proportion of women working from home increased by 23%. Millions of American workers have become accustomed to working from home and plan to continue that mode by joining the so-called "gig economy". This rapid increase in the contingent workforce has many implications for contact center performance management.

- *Persistent labor shortages:* Since the 1970s, the power of organized labor has continued to diminish. This is likely to change if the current labor shortage proves to be long-term rather than a temporary situation. According to the Bureau of Labor Statistics there were 10.4 million vacant jobs as of the end of August 2021 - far exceeding the number of job seekers. Any doubts about a labor shortage can be erased simply by looking at all the "Help Wanted" signs. Workers will require higher wages and greater flexibility. Many leading employers have voluntarily moved forward with improved wages and more flexible schedules in order to attract and retain valuable employees. Familiar names that have significantly advanced entry-level wages include Bank of America, Walmart, Costco, and Wells Fargo. Businesses that are revising their policies on flexible work include Dell Technologies, United Health Group, and American Express.

Federal Snapshot

The following are what we believe to be the most pertinent federal laws and regulations that apply to the contact center. They address three major objectives; stem abuse, prevent fraud, and protect privacy.

A short list includes:

- Telemarketing Sales Rule
- Fair Debt Collections Practices Act
- Truth In Lending Act
- Health Insurance Privacy and Portability Act
- Family Medical Leave Act
- General Data Protection Regulation (European regulation which applies to certain US companies)

The Federal Trade Commission and Consumer Financial Protection Bureau regularly releases new rulings or clarifications of prior rulings. While each of these have specific requirements that reach into the contact center, a few rules of thumb with general applicability include:

- *Be careful with personally identifiable information* - Businesses are entitled to information that is essential to their business, but this should be spelled out. The definition of PII can be very broad, particularly with certain state laws. If you think you require mobile phone numbers, email addresses, Twitter handles, or detailed information about family members you should have a written rationale for these requests and be sure to obtain the consumer's consent to collect this information.
- *Share pertinent information that consumers need to make intelligent buying decisions* - The Telemarketing Sales Rule and the Truth in Lending Act spell out details that must be shared before a sale can be executed. Scripts and compliance software are very valuable for this purpose.
- *Be respectful of individual privacy* - Telemarketing and bill collection outreaches must be limited to specific times. Telephone representatives must avoid abusive language or high-pressure techniques.
- *Prevent accidental release of inaccurate and misleading information* - With large purchases, and particularly in financial transactions conducted by phone or digital means, it is very easy for a well-meaning representative to embellish product or services benefits or misstate terms or warranties.
- *Be forthright with your privacy policies* - Businesses and organizations should clearly state their policies with regard to consumer information. The most common practice is to issue the statement on the corporate website. Additionally, businesses and organizations have a responsibility to promptly respond to customer complaints and requests regarding privacy.

State and Local

Most of the action in the state and local arena revolves around consumer privacy. The United States is unique among industrialized nations in that it does not have a national law assuring consumer privacy rights. In due time we expect there will be a national law but for now individual states are taking the initiative. Three states; California, Colorado, and Virginia have passed consumer privacy laws. States that have privacy laws under active consideration include Massachusetts, North Carolina, New Jersey, Ohio, and Pennsylvania.

Understanding these laws is important because common functions of contact center agents are to solicit new business and accept applications. Depending on the purpose, application forms can

request highly detailed personal information. It is not a violation of international or state laws to collect consumer information, but it is essential that there be a sound business purpose for collecting this data, that it is treated with the utmost security, and that consumers understand that they have the right to verify and challenge the information.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act went into effect January 1, 2020, with enforcement beginning in July 2020. The CCPA confers specific privacy rights to California residents and establishes obligations on the part of businesses that deal with private consumer information. The CCPA is aimed at for-profit entities that collect or receive personal information from California residents and meet one or more of these criteria:

(A) Has annual gross revenue that exceeds US $25 Million

(B) Annually receives, buys, sells, or shares, directly or indirectly, the personal information of 50,000 or more California residents, devices, or households or

(C) 50% or more of its annual revenue is derived from the sale of personal information about California consumers.

Personal information (PI) includes virtually any type of information which can be traced back to a specific individual. The definition of "sell" is very broad. It includes disclosing, disseminating, making available, transferring personal data, and more. Transferring consumer data from a covered entity to a subsidiary that is not covered under the law is considered a "sale" and is therefore prohibited under the CCPA. Since it does not matter where the business is headquartered, the impact of CCPA extends beyond the borders of California. This means companies can be fined or sued in California even if they are not based in California or have facilities there.

Civil penalties shall not be more than $2500 per violation or $7500 per each intentional violation. There is no maximum for multiple violations.

Consumer Rights and Business Obligations Under the California Consumer Privacy Act

- Consumers have the right to request that a business that collects personal information disclose the categories of sources from which that information was collected and the business purpose for collecting or reselling the information
- Upon request, a controller that collects personal information must delete that personal information and the business must generally comply, unless the information is essential for conducting business with the customer
- A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers of the categories of personal information that will be collected and the purposes for which the categories of personal information shall be used
- 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
- A business is required to create a separate "Do Not Sell My Personal Information" web page with a clear and conspicuous link from their homepage that informs California consumers that they may opt out of the sale of their personal information
- Consumers have the right to obtain their personal information in a format that allows them to transmit it to another organization
- Consumers have a private right of action that allows them to seek statutory or actual damages if their sensitive personal information is subject to unauthorized access, theft, or disclosure as a result of a business's failure to implement and maintain required reasonable security measures

The Virginia Consumer Data Protection Act (CDPA)

The Virginia Consumer Data Protection Act was signed into law on March 2, 2021 and goes into effect January 1, 2023. Personal data is "any information that is linked or reasonably linkable to an identified or identifiable natural person." It does not include de-identified data or publicly available information. The CDPA applies to "...persons that conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that during a calendar year, control or process personal data of at least 100,000 consumers, or control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data." The penalty is up to $7500 for each violation.

Consumer Rights and Business Obligations Under the Virginia Consumer Data Protection Act

- Consumers may request that inaccurate information be deleted
- Consumers may obtain a copy of personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to other organizations
- Consumers may choose to opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or profiling
- A controller shall respond to the consumer without undue delay. If the controller declines to act they must notify the consumer and provide justification within 45 days
- A controller shall establish a process for a consumer to appeal the controller's refusal to act on a request within a reasonable period of time after the consumer's receipt of the decision
- Consent is required to process "sensitive data"

Colorado Privacy Act (CPA)

On July 7, 2021, Colorado became the third state to pass comprehensive consumer privacy legislation, following California and Virginia. The Colorado act becomes effective July 1, 2023. It applies to businesses that process the personal data of 25,000 consumers and receive any revenue or discount from the sale of data. Personal data explicitly excludes any deidentified data or publicly available information. Civil penalties are capped at not more than $2,000 per violation and not more than $500,000 total for any related series of violations

Consumer Rights and Business Obligations Under the Colorado Privacy Act

- The right to confirm whether a controller is processing his/her personal data and to access that data
- The right to correct inaccuracies in personal data
- The right to delete personal data concerning the consumer
- The right to obtain personal data in a portable and, to the extent technically feasible, readily usable format and transmit the data to another entity without hindrance
- Businesses collecting or processing personal information must provide an accessible and clear privacy notice
- Businesses must specify the express purposes for which personal data are collected and processed
- Affirmative consent must be secured before collecting and otherwise processing "sensitive data"

Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)

The SHIELD Act's obligations apply to "Any person or business which owns or licenses computerized data which includes private information" of a resident of New York. There are exemptions for businesses with less than $3 million in gross annual revenue for each of the last three fiscal years, or less than $5 million in total assets.

Key Provisions of SHIELD Act

- Requires that any person or business that owns or licenses computerized data that includes private information of residents of New York must develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information
- Breach notification applies to any person or business which owns or licenses computerized data which includes private information of a resident of New York
- The SHIELD Act expands the definition of private information to include account numbers, credit card numbers, driver's license numbers, and biometric information, or alternatively a username or email address in combination with a password or security question
- Unless the exposure was inadvertent, notices must be sent out to affected persons
- A court may impose penalties of not more than $5,000 per violation with a cap of $250,000 for knowing and reckless violations

California Assembly Bill 5 (AB5 or "Gig Worker Bill")

The California Supreme Court has ruled that companies must use a three-pronged test to determine if an individual is an employee or an independent contractor. California later codified that ruling. The worker is NOT an employee if the following three conditions exist (known as the ABC test):

- The worker is free to perform services without the control or direction of the company
- The worker is performing work tasks outside the usual course of the company's business
- The worker is performing the job duties of their regularly established trade, occupation, or business. Sometimes there is an additional requirement which states that the contractor must be in business for themselves. This is generally proven by the contractor having, for example, a business license.

Key Provisions of California Gig Worker Bill

- Applies to freelance workers who reside in California, even if the business that hires the freelance worker is located outside of California
- Companies that hire independent contractors and freelancers must classify them as employees, unless they can prove that that three specified conditions exist
- There are notable exceptions, such as doctors, lawyers, accountants, graphic designers, and entertainers
- Freelance workers who become reclassified as employees gain various protections such as a guaranteed minimum wage and overtime pay
- Employers may not reclassify an individual who was an employee on January 1, 2019, to an independent contractor due to this measure's enactment
- Nothing in this act is intended to diminish the flexibility of employees to work part-time or intermittent schedules or to work for multiple employers
- Hiring firms that are found to have misclassified employees as independent contractors can be required to pay fines, penalties, and back pay and benefits
- California law imposes a civil penalty of up to $25,000 per violation on an employer that willfully misclassifies individuals as independent contractors

The ABC test does not apply to bona fide business-to-business contracting relationships when a contractor "acting as a sole proprietor, or a business entity formed as a partnership, limited liability company, limited liability partnership or corporation that contracts to provide services to another such business." Under AB 2257, the scope of the business-to-business exemption has been increased to include instances in which a "public agency or quasi-public corporation" has retained a contractor. AB 2257 also removes the requirement that a business service provider provide services directly to the contracting business rather than to customers of the contracting business.

California Family Rights Act (CFRA)

The California Family Rights Act requires covered employers to provide eligible employees with unpaid, job-protected leave of up to 12 weeks in a 12-month period for certain qualifying reasons. Eligible employees under CFRA are those who have more than 12 months of service and at least 1,250 hours of service during the previous 12-month period.

Significant changes became effective January 1, 2021. The most notable is that the CFRA will expand its reach to cover employers of five or more employees. Smaller employers (those with five or more employees) will be covered by the CFRA and required to provide this job-protected family and medical leave to their California employees.

Larger employers already covered by the CFRA and should also be aware of several important changes under SB 1383. Important changes include:

- Expansion of qualifying reasons for CFRA's family care leave to include more family members for whose care an employee may take CFRA leave
- Addition of "qualifying exigency" leave related to the military service of certain family members of the employee
- Elimination of an employer's ability to: (1) deny CFRA leave to an otherwise eligible employee when there are not 50 or more employees within 75 miles of the worksite; (2) refuse to reinstate a "key employee"; and (3) limit the amount of new child bonding leave to 12 weeks when both parents work for the same employer

Other Importance State and Local Laws and Regulations

- During 2021 increases in the minimum wage will go into effect in 21 states and more than 30 localities
- New paid leave initiatives to take effect in Colorado, Maine, Massachusetts, and New York
- The states of California, Nevada and Washington now require expanded training covering topics such as sexual harassment prevention, human trafficking awareness, safety, and child abuse and neglect reporting
- In Colorado the equal pay for equal work act took effect on January 1, 2021. This limits salary inquiries and requires the salary range be included on job postings
- The Chicago Fair Workweek Ordinance includes building services, healthcare providers, hotels, and manufacturers, as well as the standard retail and food service occupations. Employers must give 10 days' notice of workers' schedules. That window will rise to 14 days on July 1, 2022. Employers that make alterations to schedules after that 10-day deadline without mutual agreement to the change must pay one hour of Predictability Pay (one hour of the employee's regular rate) for each adjusted shift

Technology to Help Assure Compliance

In this brief overview we have demonstrated that there are many laws and regulations at the international, federal, state, and local levels that contact centers must be aware of and comply with. There are far too many of these for individual contact center managers or even compliance officers to be familiar with let alone manage manually. Knowledge followed by training is essential but in a fast-paced environment it is impossible to keep up with every detail. Contact centers would be well advised to invest in technology that helps to meet their compliance objectives.

The technology must be flexible, adaptable, extensible, easy to use, and compatible with the existing hardware and software. The following is a brief checklist that can help guide decision-making:

	WFM/Perf Mgmt/ Learning	Recording/Quality/ Speech Analytics
Cloud-based for agility and extensibility	X	X
Easy to use and administer	X	X
Single customer data base	X	X
Pain-free migration from current solution	X	X
Accommodates work from home workers	X	X
Accommodates contingent workforce	X	X
Mobile friendly	X	X
Empowers agents to manage their schedules	X	
Multichannel forecasting and scheduling	X	
Business planning scenarios (“what if” analysis)	X	
Incorporates employee preferences and skills	X	
Alerts for script errors, omissions		X
Identification of potential violations		X
Alerts for missed breaks or excessive hours	X	
Integrates with third-party software through APIs	X	
Encryption with multi-factor verification		X
Easy access and retrieval of requested recordings		X
Ability to quickly correct or remove consumer data	X	

We would also recommend that compliance be included as an element of the standard training regimen and also included on agent evaluation forms. Large companies will typically have a compliance department that looks at compliance from a corporate wide standpoint. This is a valuable resource. Initiatives originating at the contact center level should certainly be shared with the compliance department. However, primary responsibility for compliance remains with the contact center.

Summary

Due to underlying trends such as concerns over consumer privacy protection and growth of the contingent workforce, we are currently experiencing significant changes in the legal and regulatory environment under which contact centers must operate. On the federal front, we can anticipate that as the new administration gets its footing there will be momentum for a national privacy law, mandatory paid family leave, and clarification of the definition of the meaning and rights of contingent workers.

At the state level, the pace of new laws and regulations has been much more rapid. This complicates matters for contact center management because it is hard enough to keep up with national laws, much less, individual states and even international requirements such as the European Union’s General Data Protection Requirement.

Contact center management has to be skilled in multiple disciplines, but in-depth knowledge of pertinent laws is not one of them. If you have a compliance department and they have a good understanding of the contact center you have a valuable resource that can help you structure business rules to help assure compliance. You may also consider implementing basic protocols about the collection and storage of personally identifiable information, the wording of contracts with employees and contingent workers, scripted mandatory disclosures, and compliance as a quality evaluation criterion. Another action you can take is to invest in a suite of customer experience solutions designed with compliance as an important objective. The technology investment you make can help you avoid lapses that could prove very costly in both financial penalties and corporate reputation.

About the Author

Dick Bucci is Principal of Pelorus Associates (www.pelorusreports.com) where he specializes in contact center technologies. He has authored 19 in-depth market research reports on workforce optimization applications and numerous articles and white papers. His particular specialty is compliance. Dick has produced several white papers on laws and regulations as they pertain to contact centers and co-authored two books on public safety contact centers. He is one of a handful of industry thought leaders that have been elected to the *Contact Center Pipeline Wall of Fame*.