The Privacy Survival Guide

NEWSLETTER FROM POLSINELLI'S HEALTH INFORMATION PRIVACY AND SECURITY PRACTICE GROUP

Keeping up with the CCPA

Biometrics Developments: BIPA & Beyond

GDPR Contracting Flowchart

Maximizing Geolocation Data

Speaking

37th Annual Health Law Symposium

November 6, 2019 – Union League Club in Chicago

https://www.iahanet.org/page/2019Symposium

Concurrent II – Data Privacy and Emerging Technologies:
AI, Biometrics and Geolocation Information

Upcoming Webinars

- **Joining Law and Data Rights**
  Wednesday, August 7, 2019 | 1:00 PM ET
- **Data Innovations in Health Care**
  Wednesday, September 18, 2019 | 1:00 PM ET
- **AI and IoT: Apps, Bots, and Body Area Networks**
  Wednesday, November 13, 2019 | 1:00 PM ET

Keeping up with the CCPA

Privacy Officers, General Counsels, Compliance Officers, and Chief Information Officers across the country are actively monitoring developments surrounding the California Consumer Privacy Act (CCPA). With pending proposed legislation and amendments, preparations for compliance with the CCPA will require flexibility leading up to the CCPA's January 1, 2020 effective date.

Despite uncertainty surrounding the CCPA, beginning an internal compliance assessment can serve as both a roadmap and a building block for your company's compliance program. The key principles and foundations of the CCPA align with other privacy laws in the United States, the European Union (e.g., GDPR), and across the globe. Accordingly, the early stages of a CCPA compliance program can refresh privacy perspectives in a streamlined and efficient manner.

This article provides an overview of the existing legal landscape and pending amendments and breaks down the CCPA into phases and workstreams which can be implemented at your company.

The Whom it Applies
CCPA applies to companies who collect information about California residents and who meet at least one of the following thresholds (which are intended to exclude smaller-scale companies):

- Annual gross revenue over $25 million; or
- Collects or buys information about more than 50,000 individuals; or
- Derives at least 50% of its revenue from selling consumers' information.

The What It Currently Requires
The CCPA requires these companies to:

1. Lawfully use personal information (which is defined very broadly to even include information "that is capable of being associated" with a particular person);
2. Maintain "reasonable security procedures" based on the types of personal information collected; and
3. Respect and comply with residents' requests to exercise rights granted to them by the CCPA.

Rights Created by the CCPA	
Transparency	Identification and discloses to consumers of the information being collected and the purpose of information collection.
Access	Consumers have the right to access the information a company collects and maintains about them.
Opt-Out	Consumers are able to opt-out of having their information sold.
Deletion	Consumers can have their information deleted (in some circumstances).
Portability	Consumers have a right to get a copy of the information a company has about them.
Equal Service	Companies cannot discriminate against consumers who exercise their rights, including access to information rights.

CONTINUED ON PAGE 3

CONTINUED FROM PAGE 2

The When

The CCPA is scheduled to go into effect on January 1, 2020. However, there are many proposed amendments which could significantly impact the scope of the CCPA's legal requirements. Just some of these amendments include:

Amendment	Amendment's Impact
AB 25	Removes employment data from the law's scope.
AB 846	Allows for differential treatment if it is based on the consumer's voluntary participation in a loyalty reward or discount program or if they enroll in a premium feature in exchange for sharing their data.
AB 873	Modifies the definition of "personal information" to be information that is "reasonably capable of being associated with" an individual. It would also change the definition of "deidentified" information to be information that is not reasonably linkable to an individual.

The How

Below is a breakdown of compliance activities into four different phases, which would allow your organization to start tackling the CCPA without being derailed by future changes in the law.

Phases	Planning	Data Gathering Activities	Assessment & Gap Analysis	Implementation & Remediation
Activities	• Analysis of how and why CCPA applies to the company • Draft Project Work Plan • Review existing data inventories/maps for CCPA relevancy • Develop interview questionnaire • Identify preliminary set of questionnaires for recipients and other stakeholders • Schedule stakeholder meetings (in person or by phone)	• Conduct data mapping • Submit and get responses to questionnaires • Identify all vendors and third parties that receive data and contacts for each • Collect existing policies, procedures and practices • Commence onsite visits and/or stakeholder telephone interviews	• Cross-reference statutory requirements to current policies, procedures and practices • Assess vendor contracts • Perform gap analysis • Prepare Compliance and Risk Report • Develop prioritized remediation plan • Create an action plan and supporting documentation	• Update and develop new processes • Update and draft new policies and procedures • Update disclosures and consent documents • Revise and/or put in place vendor contracts
Deliverables	1. Meeting Materials & Work Plan 2. Interview questionnaire 3. Stakeholder interview schedule 4. Weekly Status Meetings and Reporting Template	1. Completed data map 2. Completed gap analysis questionnaires 3. Stakeholder interview notes	1. Compliance-Readiness Findings 2. Gap Analysis Results 3. Compliance and Risk Report 4. Remediation and Action Plans	1. Same as above

CONTINUED ON PAGE 4

CONTINUED FROM PAGE 3

Next, divide up the CCPA requirements into six discrete work streams:

Workstream	Description
Data Mapping	• Review/update Personal Information inventories and flows to understand what Personal Information is being processed, for what purposes, where and who has access
Vendor Review	• Identify vendors/service providers to whom Personal Information is transferred, how such Personal Information is used/further shared/sold • Review and revise contracts • Diligence to ensure consumer right fulfillment mechanisms
Consumer Request Fulfillment	• Review systems and operations to ensure ability to comply with data subjects' requests • Provide opt-out mechanism and rights request channels • Establish policies and procedures for data subject requests, including identity verification
Privacy Disclosures	• Update privacy policy disclosures and ensure proper notifications are provided prior to collection of Personal Information
IT Security	• Review systems and operations to ensure appropriate encryptions used for data • Establish and document data retention policies for each category of data to ensure data minimization
Ongoing Compliance	• Establish training program and update/establish appropriate internal compliance policies and procedures

Biometrics Developments:
BIPA & Beyond

Biometric Information Privacy

As companies across all industries continue to collect and utilize a wide range of personal information, biometric data has become an increasingly popular identifier to utilize in the workplace, especially for health care providers. For example, long term care facilities are implementing biometric timekeeping systems for their employees, and hospitals are using biometrics to identify their patients.

Three states in the United States currently have statutes entirely dedicated entirely to biometrics – Illinois, Washington and Texas. The most stringent of the three is Illinois' Biometric Information Privacy Act (BIPA), which was recently interpreted by the Illinois Supreme Court found that the plaintiff did ***not*** need to allege actual harm in order to be considered an aggrieved party under the BIPA. Federal lawmakers also have taken a recent interest in biometric privacy, a bill introduced in March would require companies to obtain consent prior to sharing facial recognition data, and impose a variety of other limitations on the use of facial recognition technology. Any company collecting or using biometrics should be aware and monitoring legal developments to understand the necessary compliance measures which may be required.

Illinois' Biometric Information Privacy Act (BIPA)

BIPA is currently the most stringent statute in the nation regulating biometric identifiers and information. It was enacted in response to the growing use and recognition that biometrics are unlike other unique identifiers, especially when used to access finances or other sensitive information. BIPA does the following:

- BIPA applies to any "Private entity," which means any individual, partnership, corporation, limited liability company, association, or other group, however organized (excludes government agencies);

CONTINUED ON PAGE 5

CONTINUED FROM PAGE 4

- Creates a private right of action for aggrieved persons, with damages ranging from liquidated damages of $1,000 or actual damages for a negligent violation (whichever is greater), to liquidated damages of $5,000 or actual damages for an intentional or reckless violation (whichever is greater); and
- Allows for attorney's fees and litigation costs or other relief, including an injunctive relief.

Recent Developments

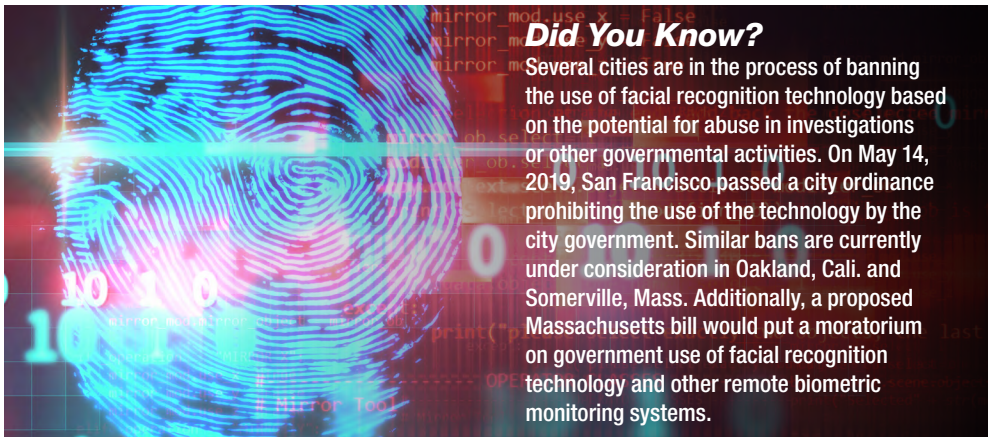
In *Rosenbach v. Six Flags*, a plaintiff alleged that Six Flags improperly collected the thumbprints of their son when he purchased a season pass for the theme park on a school field trip. There were no allegations that the thumbprints were stolen or misused, rather the complaint alleged Six Flags violated BIPA due to:

1. Not obtaining a written release before collecting biometric data;
2. Not informing that biometric data would be collected and stored, or for what purpose; and
3. Not stating the length of time the biometric data would be kept or used.

Six Flags argued the plaintiff did not have a claim under BIPA because there were no allegations of harm resulting from the collected thumbprints and, therefore, the plaintiff did not have standing as an "aggrieved person" under BIPA. Six Flags relied on an Illinois Appellate Court decision that indicated a mere technical violation of BIPA alone was not sufficient to pursue damages, but rather an injury or adverse effect must actually be alleged.

However the Illinois Supreme Court rejected this argument, finding that an "aggrieved person" under BIPA does not need to have "sustained actual damage beyond violation of his or her rights under the Act in order to bring an action under it," reasoning that **the Illinois legislature enacted BIPA to safeguard biometric privacy rights before they can be compromised.**

This decision is important for companies collecting biometric data, as an increasing number of companies elect to utilize biometric data to create efficiencies and improve their services. An increasingly popular example is companies using biometrics for timekeeping purposes so employees can clock in and out more accurately. Several class action suits have been filed challenging this practice, including one currently pending in federal court against Southwest Airlines. To that care, where employees are challenging the airline's requirement that employees clock in and out using their fingerprints.



Did You Know?

Several cities are in the process of banning the use of facial recognition technology based on the potential for abuse in investigations or other governmental activities. On May 14, 2019, San Francisco passed a city ordinance prohibiting the use of the technology by the city government. Similar bans are currently under consideration in Oakland, Cali. and Somerville, Mass. Additionally, a proposed Massachusetts bill would put a moratorium on government use of facial recognition technology and other remote biometric monitoring systems.

Proposed Federal Law

Companies collecting biometric data should track federal legislation that may impact their use of biometric information. **The Commercial Facial Recognition Privacy Act, introduced in March 2019, requires companies to first obtain consent prior to using facial recognition technology,** in addition to a variety of other measures to help consumers maintain autonomy over their biometric data, specifically images of their faces. Companies would also be required to:

- Notify individuals when their facial recognition data is used or collected;
- Provide, if contextually appropriate, where the individual can find more information about the use of facial recognition technology; and
- Provide documentation and general information that explains the capabilities and limitations of facial recognition technology in terms that individuals can understand.

The legislation would also provide additional protection to individuals whose biometric information is collected by prohibiting the use of facial recognition technology to discriminate against an end user in violation of applicable federal or state law. Users of facial recognition technology would be prohibited from repurposing facial recognition data for a purpose that is different from that initially presented to individuals, and also from sharing the data with unaffiliated third parties without consent.

Key Takeaways

Using biometrics can be an easy solution for companies to employ and solve a variety of everyday tasks: clocking in and out of work; unlocking a phone; or authenticating identities. The ease associated with swiping a fingerprint or using facial recognition is not without risk, however. Companies utilizing biometric technologies should balance the benefits of utilizing this of technology against the burdens associated with legal compliance in certain jurisdictions. In Illinois, this means:

- Obtaining consent from individuals;
- Developing a written policy establishing guidelines for the collection and destruction of biometric data;
- Establishing a retention schedule and guidelines for destroying biometric identifiers; and
- Informing individuals not only of the collection, but also what collection is being used for and how it is being retained (including the length of time that biometric data is being stored).

GDPR Contracting Flowchart

This purpose of this Flowchart is to identify when a Data Protection Agreement (DPA) is required by the General Data Protection Regulation (GDPR), and then to determine the role that each party plays when providing the underlying services. Capitalized terms used in this Flowchart have the same meanings as those terms defined by the GDPR.

Step #1: Is a DPA required? A DPA is required when all four components are present as outlined below.

Personal Data	• Name, email, health data, social security number, location or identification device • Political opinion, race, ethnicity, genetic or financial information
Data Subjects	• Patients, employees, applicants, health care providers • Located in the European Union/European Economic Area
Processing	• Collecting, recording, storing, retrieving, using, disclosure • Transmitting, erasing, destroying, aligning, combining
Controller & Processor	• Controllers determine the purposes for Processing Personal Data • Processors act on the instructions of the controller

A DPA is ***not*** required when Personal Data is not processed to perform the underlying services, or if both parties are Controllers.

Step #2: Who is the Controller vs. Processor? Examine the underlying services and processing activities to determine each party's role.

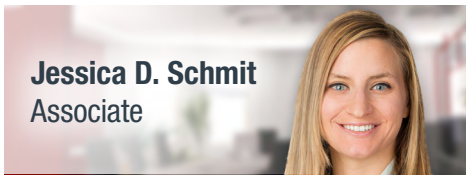
Controller

- Alone or jointly with others, determines the purposes and means of the **Processing of Personal Data.**
- Carries out **Processing** activities such as interpretation, the exercise of professional judgment or significant decision-making in relation to **Personal Data.**
- If an entity is required by law to process **Personal Data,** it must retain its status as a **Data Controller** and assume responsibility for the **Processing.** For example, if Entity A hires a third party to fulfill its own legal obligations to its employees (such as hiring an external accountant to assist with calculating salary or hiring a vendor to do specific trainings for employees), Entity A is the **Data Controller.**
- If an entity makes decisions regarding **Personal Data** which demonstrate its overall control of the Processing, then that entity is likely the **Data Controller.** Some of these decisions may include:
  - To collect the **Personal Data** in the first place and the legal basis for doing so;
  - Which types of **Personal Data** to collect;
  - The purpose(s) the **Personal Data** is to be used for;
  - Who to collect **Personal Data** from;
  - Whether to disclose **Personal Data,** and if so, to whom;
  - Whether **Data Subject** access and other rights apply; and
  - How long to retain the data or whether to make non-routine amendments to **Personal Data.**

Processor

- **Processes Personal Data** on behalf of a **Data Controller.**
- Carries out **Processing** activities which are more limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure.
- Typically only makes some decisions regarding **Personal Data** similar to the below items:
  - What IT systems or other methods to use to collect **Personal Data;**
  - How to store **Personal Data;**
  - The detail of the security surrounding the **Personal Data;**
  - The means used to transfer the **Personal Data** from one entity to another;
  - The means used to retrieve **Personal Data;**
  - The method for ensuring a retention schedule is adhered to; and
  - The means used to delete or dispose of **Personal Data.**

Maximizing Geolocation Data



Health care providers are looking to connect with patients in innovative ways and create a more personalized patient experience. Location-based services are a useful and well-established technology in other industries, but the application to health care is relatively new and complex. Today's health care providers are looking to engage patients and increase brand awareness through location technologies by offering driving directions to their facilities through their website and app, or by creating proximity-based marketing campaigns and encouraging social media "check ins."

Geolocation information typically refers to information which can be generated or derived to determine the precise location of a device or individual. Until recently, there has been very little regulation addressing the collection and use of geolocation information. A bill currently pending in Oregon attempts to do just this and regulate geolocation information, an initiative other states have attempted to do but without success. In 2014 the Federal Trade Commission (FTC) testified on the sensitivity inherent in tracking location information, noting in its **press release** this can raise concerns because "precise geolocation data is sensitive personal information increasingly used in consumer products and services … these products and services make consumers' lives easier and more efficient, but the use of geolocation information can raise concerns because it can reveal a consumer's movements in real time and provide a detailed record of a consumer's movements over time." The **testimony** further stated:

> ***"Geolocation information can divulge intimately personal details about an individual. Did you visit an AIDS clinic last Tuesday? What place of worship do you attend? Were you at a psychiatrist's office last week? Did you meet with a prospective business customer?"***

New Proposed Law in Oregon

Oregon is the most recent state to attempt to regulate the collection of geolocation information through a proposed amendment to its Data Transparency and Privacy Protection Act, introduced this February as **House Bill 2866**. This proposed amendment would require express written consent prior to collecting, using, storing, analyzing, deriving inferences from, selling, leasing or otherwise transferring geolocation information (defined as "data that displays the location of a digital electronic device on a map or similar depiction with an accuracy that is sufficient to correctly indicate the device's actual spatial location within a radial distance of 1,500 feet or less, but does not include an Internet Protocol address that is not combined with any other data that would indicate the spatial location of the digital electronic device that is using the Internet Protocol address). Companies would also be required make certain disclosures at a resident's request, and without charge, regarding the geolocation information collected about them. Those who fail to comply will be deemed as engaging in unlawful trade practices under Oregon law and subject to penalties.

Past Privacy Initiatives

Over the years, federal and state legislatures have attempted to regulate geolocation information in a variety of ways:

1. The Massachusetts Attorney General issued a no-fault settlement to a digital advertising company hired to establish geofences around reproductive health facilities and then send targeted ads to women visiting these facilities. The Massachusetts Attorney General barred the advertising company from using "geofencing technology at or near Massachusetts health care facilities to infer the health status, medical condition, or medical treatment of any individual."
2. Illinois tried to pass a Geolocation Privacy Protection Act in 2017, but it was ultimately vetoed by the Governor at that time.
3. A federal Geolocation Privacy and Surveillance Act was introduced to give commercial entities and private citizens clear guidelines for when and how geolocation information can be accessed and used. It would have also prohibited businesses from disclosing geographical tracking data about its customers to others without the customers' permission, but it has seen no further movement.

CONTINUED ON PAGE 8 ▸

CONTINUED FROM PAGE 7

Things to Consider

It can be challenging for an organization interested in leveraging geolocation information to know whether it is operating within the confines of the law, so monitor the following types of legal developments:

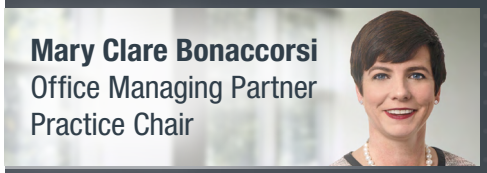
- State breach laws, which may include geolocation or other location information as an identifier;
- State consumer privacy laws, which may place restrictions on how geolocation information may be used and disclosed; and
- State geolocation privacy laws, such as Oregon's pending legislation, which specifically restricts when entities may collect and otherwise use individuals' geolocation information.

While the possible uses of geolocation information are seemingly endless, those uses present risks, especially in light of an ever-changing and murky legislative landscape. Health care companies interested in hiring a third party to utilize this type of information should consider the following best practices:

- Monitor any legal developments in this area and proceed with caution;
- Obtain representations and warranties that third parties will comply with all applicable current and future laws impacting location information;
- Confirm appropriate safeguards that are utilized to securely collect and store the information; and
- Ensure third parties have the ability to immediately turn off location data collection in the event of a significant legal change.

Contacts for More Information

Lisa J. Acevedo
Shareholder
312.463.6322
lacevedo@polsinelli.com



Mary Clare Bonaccorsi
Office Managing Partner
Practice Chair
312.463.6310
mbonaccorsi@polsinelli.com

Lindsay R. Dailey
Associate
312.873.2984
ldailey@polsinelli.com

Colleen M. Faddick
Shareholder
Practice Chair
303.583.8201
cfaddick@polsinelli.com

Kathleen D. Kenney
Shareholder
312.463.6380
kdkenney@polsinelli.com

The explosion of digital data, along with the proliferation of technology, devices and other health care innovation has created a multi-layered range of privacy and data security issues in the health care industry. Polsinelli's multi-disciplinary Health Information Privacy and Security Team brings together attorneys across the firm specializing in the areas of privacy, security, technology and litigation, who understand the value of your health-related data and are adept at assisting clients in maximizing the benefits of that data while minimizing and responding to ever-changing threats and risks.

Our team has deep experience in the full breadth of privacy/security-related laws and regulations impacting the health care industry, including HIPAA, FERPA, federal laws and regulations governing the confidentiality of alcohol and drug abuse treatment records, state privacy/security laws related to the confidentiality of health information (including mental health, HIV/AIDS and genetic information), and international privacy laws impacting data use and transfers.