TRUSTPOINT.ONE WHITEPAPER

The American Data Privacy and Protection Act:

What is it? Why should my organization care?

Introduction

The United States is different than most countries in how we deal with data privacy. Other countries with data protection laws, such as Brazil, have created nation-wide laws that protect personal and sensitive information. In the United States, we have a mix of federal and state laws covering various areas of data privacy. Some of the previous federal laws, like the Health Insurance Portability and Accountability Act, cover certain areas in protecting personal information, such as health, education, and finance. These federal laws are very specific to their application, but do not address the protection of overall data privacy – that's left up to the states. State privacy regulations are all over the place in that some are much more detailed than others.

There have been many attempts in the past to have a federal law created to help businesses and bring the country to one standard in regards to data protection, but each time has been shut down. Now, we are seemingly closer than ever to having a comprehensive federal data privacy law with the American Data Privacy and Protection Act.

What is the American Data Privacy and Protection Act?

The American Data Privacy and Protection Act (ADPPA) was first introduced in June of 2022. It has quickly garnered bi-partisan support and has gone through several major hurdles. Having gone through the House Energy and Commerce Committee, it has done so with nearly full support from Congress. With no current comprehensive federal data privacy regulations, this act is the leading edge of protecting personal and sensitive information at a nation-wide level. The latest version includes items such as data minimization, controls for large data holders, additional individual privacy rights, and cut outs for third-party data collectors whose sole business is to collect data and sell that information. Some of these items will be brand new data privacy concepts for organizations to consider.

What are some ways that ADPPA will affect organizations?

Oftentimes, companies collect personal and sensitive data on individuals without even knowing that the information is protected or could become protected. These same organizations often store this information indefinitely through backups on devices like hard drives, thumb drives, and even the cloud. ADPPA addresses the over-collection of personal and sensitive information and holds those that store masses of it accountable. The proposed act will apply to "Covered Entities", which the act currently defines as collects, processes, or transfers covered data and is subject to the jurisdiction of the Federal Trade Commission (FTC), including nonprofits and telecommunications common carriers. "Covered Data" is further defined as information identifying, linked, or reasonably linkable to an individual or device linkable to an individual. These definitions cover almost all organizations, nonprofits, and institutions.

Similar to the comprehensive data protect and privacy laws in Europe, the proposed act gives consumers (individuals) rights to hold organizations accountable for collecting and storing their personal information.

Consumer Controls and Access

Similar to the comprehensive data protect and privacy laws in Europe, the proposed act gives consumers (individuals) rights to hold organizations accountable for collecting and storing their personal information. This includes the right to access, correct, or delete their personal information. This means, on request, the organization will need to provide all personal data that it has on a certain individual, the individual will need to be able to correct incorrect personal information, and the organization will need to be able to delete the individual's personal information. The current version does have a few exceptions to meeting these requests, such as if the requestor's identification cannot be verified, or if the request is impossible or impractical.

Organizations will need to understand what data they have and where it's stored in order to reply to requests for access, correction, or deletion. Without this understanding, they could find themselves out of compliance if a request was made by an individual on the personal data held by the company.

There are several approaches that an organization may take to getting ahead of any federal comprehensive data privacy law. To start, they need to understand ***what type of data they have and where it's located.***

Data Minimization

The ADPPA calls data minimization one of a company's "duties of loyalty." This means an organization will not collect more information than is needed and that is proportionate to the service that is being provided. Additionally, if a company needs to collect more information than needed, the act has listed seventeen permissible purposes of when this additional collection is allowed.

Organizations will need to adjust their privacy policies in order to meet the proposed data minimization requirement and make sure they are not collecting unnecessary information on individuals. Additionally, companies may need to take further safeguards that go beyond the act in protecting the data, such as adding additional access controls to certain data or shortened retention policies, and ensure they are not collecting additional personally identifying material.

Large Data Holders

The ADPPA has created a new category for organizations that hold a lot of personal and sensitive information. This regulation is mostly targeted at social media platforms and those in the practice of collecting data on individuals as their primary business. Congress has created sixteen different categories in what it considers "sensitive covered data" that these organizations will need to consider.

A large data holder will have to give additional safeguards for the information, in addition to disclosures to the individuals from whom it is collecting the information. The act would also require these organizations to have privacy officers and data security officers that would report on their compliance, perform reviews of their privacy policies, conduct trainings, audit their privacy programs, and serve as a point of contact between the large data holder and the enforcement authority.

Third-Party Personal Data Collection

In the current draft of the act, there is a section addressing third-party collecting entities. These entities are those whose main source of revenue comes from processing or transferring data that they do not directly collect from consumers. There would be additional requirements for these organizations to comply with FTC auditing regulations, and if they meet a certain threshold, they would have to register with the FTC. Those that are on this registry would be subject to not collecting information on individuals that join a "Do Not Collect" list.

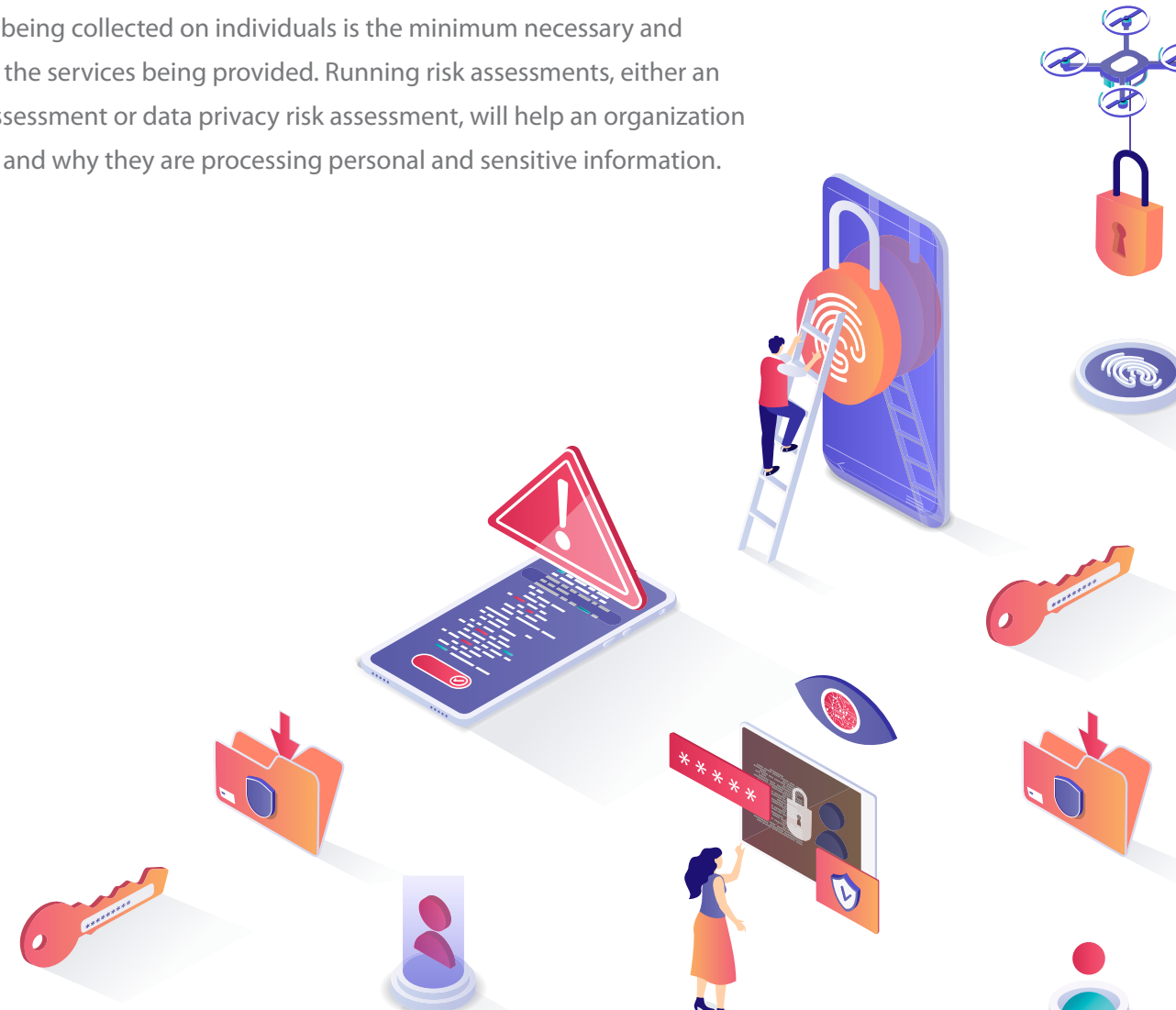
Similar to the "Do Not Call" regulations, third-party collecting entities will also need to establish mechanisms to ensure they are not holding information on an individual that is on the "Do Not Collect" list.

What can an organization do now to get ahead of a federal comprehensive data privacy law?

There are several approaches that an organization may take to getting ahead of any federal comprehensive data privacy law. To start, as part as a best practice for organizations, they need to understand what type of data they have and where it's located. Running a data mapping exercise to identify and locate personal and sensitive information that an organization may be storing will pay dividends if a federal comprehensive data privacy law is passed. The results of a data mapping exercise would help facilitate changes to privacy policies and compliance with any new federal data privacy law.

In addition to running data mapping exercises, companies should look at why and how they are processing any personal and sensitive information to make sure they are not holding onto information that is unnecessary. As we see in the draft of the act, and discussed above, part of the duty of loyalty is data minimization. So, understanding why and how the data is being used will help a company ensure that information being collected on individuals is the minimum necessary and proportionate to the services being provided. Running risk assessments, either an overall privacy assessment or data privacy risk assessment, will help an organization find out the how and why they are processing personal and sensitive information.

Companies should look at why and how they are processing any personal and sensitive information to make sure they are not holding onto information that is unnecessary.



What are some of the hurdles of the act?

As this act moves through Congress and prepares for a vote, there are two items that are still being debated—a private right of action and federal preemption.

Private right of action

In the past and in most state law regulations regarding data privacy, it was up to the state attorney general to bring action against a company in the event of a data breach. In many states, an individual is not able to bring a privacy right of action in the event of a data breach. In the current draft of the act, there would be a private right of action for violations of this act, which would include data breaches.

Congress will have to balance the accountability of compliance of the act for businesses and the consumer's rights. It is looking at limitations and/or delays in installing the law's enactment for businesses to have time to become compliant, among other considerations.

Federal preemption

One item that act addresses is to ensure that its provisions and regulations supersede those of similar state laws. The reason for this is that businesses are already spending many resources to become compliant with all of the different state regulations. Part of the reason for this act is to give organizations an easier path for compliance in taking a singular, holistic approach. Having to still comply with the varying state laws could hinder that effort. States such as California, which has some the most stringent data privacy laws, are arguing that this act will render their data privacy laws useless. The Attorney General of California, among nine other state attorneys general, have sent Congress a letter expressing that the act would set a "ceiling" rather than a "floor."

Congress will have to navigate this issue in order to convince the state attorney generals that this act is indeed a floor, as opposed to ceiling, and sets a federal standard for organizations to come into compliance that they can build upon.

Jerry McIver,
Director Trustpoint Cyber Services

www.trustpoint.one