Fair Information Practice Principles

The Fair Information Practices Principles form the backbone of privacy law in the United States and the concepts they include have played a significant role in the development of data protection laws around the globe. Understanding the Fair Information Practice Principles and how they should be implemented is critical to comply with the various privacy laws that protect personal information.

**The Fair Information Practice Principles**

*Notice/Awareness*

Individuals should receive notice of an entity’s privacy practices prior to the collection of personally identifiable information. Notice allows individuals to make informed choices regarding the use of the personal information. A privacy notice must include:

- A legitimate name and physical address of the entity collecting the data
- The type of data collected
- How collected data will be used
- Any potential third party disclosure of personal information
- Any potential secondary use of personal information

*Choice/Consent*

Individuals must be able to consent or reject to certain uses of their personal information, particularly with regard to secondary uses and marketing purposes. Two main mechanisms are used to provide consumer with consent options:

- **Opt in**: Require affirmative consent from the individual. In other words, action must be taken by the individual to START the processing of personal information for secondary uses or disclosures. This may include signing up to receive marketing newsletters, special offers and similar types of communications.
- **Opt Out**: Requires the implicit consent of the individual. Here consent is assumed because the individual has not stated a desire otherwise. In other words, action must be taken by the individual to STOP the processing of personal information for secondary uses or disclosures. This may include opting out of third party advertising

An individual must be able to view their consent options and change them at any time. Changes should be honored within a reasonable length of time.

*Access/Participation*

An individual must be able to view the data an entity has on record. They must also be allowed to correct an incomplete or false information contained in their file. Access to data must be granted within a reasonable time frame and at a minimal cost.

*Integrity/Security*

Data must be accurate, up-to-date, complete and not stored longer than necessary. Security of data must be maintained using physical, technical and administrative safeguards to protect against unauthorized access, use, disclosure and destruction. Safeguards should be implemented in proportion to the security risk or threat, with greater risks or threats using greater resources and stronger protections.

*Enforcement/Redress*

An individual must be able to file complaints with the entity have their issues addressed. Furthermore there should be a mechanism in place to ensure compliance with the above standards, either through self or government regulation.

**Enforcement of Privacy Practices**

The Fair Information Practice Principles are suggestions to guide the use of personal information in connection with business activities and transactions. They are not in themselves a law that must be followed, and as such are not enforceable. However, there are many privacy laws(see below) which make use of the Fair Information Practices to protect personal information.

The United States supports the use of self-regulation to enforce Fair Information Practices. Theoretically, informed consumers will choose to use businesses that implement the Fair Information practices and ensure the protection of their information, forcing those business that do not guarantee such protections out of business. Services such as the Better Business Bureau and online assurance programs build trust between businesses and consumers by providing consumers with a directory of businesses whose privacy practices have been assessed and found to provide adequate protection.

The Fair Information Practice Principles have been criticized because they do not require the creation of a general privacy authority and rely largely on self-regulation, which at times falls short of adequately regulating consumer protection. At the same time, many businesses believe implementing stronger guidelines or regulations would be too costly and detrimental to the growth of business. For now, the United States continues to use a sectoral approach, developing privacy laws as needed.
Laws Using the Fair Information Practice Principles to regulate Privacy

- **Fair Credit Reporting Act**– Regulated by the Federal Trade Commission, the Fair Credit Reporting Act regulates the use of consumer reports. Requires Notice of disclosure and adverse action, as well as the ability for a consumer to access and rectify inaccuracies in their consumer reports.

- **Right to Financial Privacy Act**– Protects the privacy of customers using financial institutions from government searches (with exceptions.) RFPA restricts government access to financial records without the individual’s consent or meeting one of the specified exemptions from the rule.

- **Children’s Online Privacy and Protection Act**– Protects against the collection, use and disclosure of the personal information of children under 13 without parental notice and consent.

Summary:

The Fair Information Practice Principles form the backbone of privacy laws in the United States. Though the principles put forth by the FTC are only considered guidelines, there are some laws that have turned the guidelines into law and even more businesses which choose build trust with consumers by ensuring their privacy through self regulation of the Fair Information Practice Principles. Understanding the principles and their implementation is one of the core concepts all privacy professionals need to know.

CIPP/G Candidate Preparation

In preparation for the Certified Information Privacy Professional Government exam, a privacy professional should be comfortable with topics related to this post including:

- Privacy Principles and Definitions including Fair Information Principles(I.B.a.i.)

Is Your New Health Start Up Outside HIPAA? | Privacy Analytics

May 21st, 2014 at 11:51 am

[...] of the FTC Act. You should also be aware of FTC expectations and best practices regarding Fair Information Privacy Principles. Other federal privacy laws you need to evaluate include CAN-SPAM (email marketing), COPPA [...]

https://www.cippguide.org/2010/01/18/fair-information-practices-principles/