OURY LAW

Data Protection in the U.S.

A WOLF IN SHEEP'S CLOTHING

Introduction

The U.S. currently does not have a single, comprehensive federal law regulating privacy but there are many federal laws that regulate the collection, use, processing, disclosure, and security of personal information. Overseas companies entering the U.S. market face the specter of U.S. government-imposed civil and criminal sanctions, private lawsuits and damage to a company's reputation and customer trust.

Broad Federal Consumer Protection

The Federal Trade Commission (FTC) Act prohibits the use of *unfair* or *deceptive practices* in the collection, use, processing, protection, and disclosure of personal information. The FTC Act does not regulate specific categories of personal information but instead prohibits unfair or deceptive acts or practices that fail to safeguard consumer's personal information.

Who Does It Apply To?

The FTC does apply to most companies and individuals doing business in the U.S.

Examples of enforcement action include:

- Failing to comply with statements in posted privacy policies;
- Material changes to privacy policies without adequate notice to consumer; and
- Failing to provide reasonable and appropriate security measures for sensitive consumer information.

Facebook was fined $5Bn in mid-2019 for deceiving users about how much control they have over their privacy.

Uber settled with FTC in 2018 for failing to safeguard 25.6m customer accounts. They agreed to implement a comprehensive privacy program and 20 years of biennial independent assessments.

Special Rules for Commercial Websites And Mobile Apps Directed at Children Under 13[i]

Here companies must provide a privacy notice, obtain verifiable parental consent and maintain procedures to ensure the confidentiality, security and integrity of the personal information collected. In September 2019 YouTube was fined $170m for collecting children's personal information without proper notice and verifiable parental consent.

Different To GDPR?

The FTC does not require a company to have a Privacy Notice, nor does it address consent nor does it provide specific rights to access or correct personal information.

The FTC does not address data security, but the FTC has taken enforcement action where a company has failed to take reasonable and appropriate steps to protect personal information. Inadequate data security can form the basis for a deceptive practices claim.

INDUSTRIES WITH SPECIFIC FEDERAL LAWS

Financial[ii]
Healthcare[iii]
Telemarketing[iv]
Commercial email[v]

What Should I Do?

The FTC has issued legally non-binding best practice guidance.

In March 2012 the FTC issued "Protecting Consumer Privacy in an Era of Rapid Change," which detailed recommendations for best privacy practices for companies, including use of privacy-by-design principles.

In 2009 the FTC published "Self-Regulatory Principles for Behavioral Advertising," which discussed tracking an individual's online activities to deliver tailored advertising, expanding this to mobile in 2015.

In 2017 the FTC issued a report on cross-device tracking recommending transparency, consumer choice, and reasonable security.

The FTC regularly publishes data security guidance.

States That Have Adopted Privacy and Data Security Laws

California and Massachusetts were early adopters of the most rigorous state-level privacy and data security laws.

[i] Children's Online Privacy Protection Act
[ii] Gramm-Leach-Bliley Act
[iii] Health Insurance Portability and Accountability Act
[iv] Telephone Consumer Protection Act
[v] Controlling the Assault of Non-Solicited Pornography and Marketing Act