GUNSTER

FLORIDA'S LAW FIRM FOR BUSINESS

Privacy Regulation and Enforcement in the United States

Bill Dillon
Board Certified in Health Law
CIPP/US

GUNSTER

Sectorial Privacy in the United States

- Unlike the European Union and many other countries, the US does not have a single overarching privacy law.
- In fact, the US has a large number of privacy laws at both the state and federal level (many of which are inconsistent with each other) which are enforced by a disparate group of government regulators.

GUNSTER

Regulated Privacy Sectors

- The following is a non-exclusive list of privacy sectors that are regulated and subject to regulatory enforcement.
  - Health Care
  - Financial
  - Education
  - Telecommunications and Marketing
  - Online Activities
  - Work Place
  - Legal Services

GUNSTER

Health Care

- Most Common Health Care Sector Laws with Privacy Components
  - Health Insurance Portability and Accountability Act of 1996 (“HIPAA” not “HIPPA”)
  - Genetic Information Nondiscrimination Act of 2008 (“GINA”)
  - Substance Use Disorder – 42 CFR Part 2
  - Privacy Act of 1974 (VA and Indian Health Services)
  - 21st Century Cures Act – Information Blocking
  - Others

GUNSTER

Financial Sector

- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act
- The Fair Credit and Accurate Transactions Act
- Privacy Act of 1974 – SEC new rules September of 2023.
- Others
  - Payment Card Industry Data Security Standard*

*Private industry group that sets member security standards to promote secure payments

GUNSTER

Education Sector

- Family Educational Rights and Privacy Act (FERPA) – Federal law that protects the privacy of student records. The law applies to all schools that receive Federal education funds.

GUNSTER

Telecommunications and Marketing

- Telephone Consumer Protection Act – Restricts the making of telemarketing calls and the use of automatic dialing systems. Revised in 2012 to require telemarketers to get express consent and provide a mechanism to opt-out of calls.
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM" Act) – deals with unsolicited commercial emails and texts.

GUNSTER

- Telecommunications Act of 1996 – Privacy component deals with the use of customer data obtained by telecommunications carriers.
- Cable Television Privacy Act of 1984 – Requires cable companies to notify customers on the ability to collect and use the customers' personal information.
- Video Privacy Protection Act of 1988 – Limited video tape rental information (Supreme Court Nominee Robert Bork)
- State Laws

GUNSTER

Work Place

- Large number of laws designed the protect employees that also have a privacy component:
  - Civil Rights Act of 1964
  - Pregnancy Discrimination Act
  - Americans with Disabilities Act
  - Age Discrimination in Employment Act
  - GINA
  - HIPAA
  - COBRA
  - ERISA
  - FMLA
  - FCRA
  - FLSA
  - OSHA
  - NLRA
  - Other Federal and State

GUNSTER

Legal

- Client privacy obligations imposed by the various State Bar rules
- Florida Bar Rules
  - 4-1.6(a) – Consent Required to Reveal Information
    - Acting Competently to Preserve Confidentiality Paragraph (e) requires a **lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties** and against inadvertent or unauthorized disclosure by the lawyer or other persons who are RRTFB August 21, 2023 participating in the representation of the client or who are subject to the lawyer's supervision
    - Florida Bar Ethics Opinion 20-01 (Negative online reviews)
    - Florida Bar Ethics Opinion 12-3 (Cloud computing)

GUNSTER

Comprehensive State Privacy Regulations

- California
  - CCPA (2020)
  - CPRA (2023)
- Colorado (2023)
- Connecticut (2023)
- Delaware (2025)
- Indiana (2026)
- Iowa (2025)
- Montana (2024)
- Oregon (2024)
- Tennessee (2025)
- Texas (2024)
- Utah (2023)
- Virginia (2023)

GUNSTER

Other State Related Privacy Regulations

- Several of states have more limited privacy related regulations
  - Florida Digital Bill of Rights
    - (Applicable to consumers but regulation is limited to data controllers that among other conditions have annual gross revenues exceeding $1 billon dollars.)
- All 50 states do have data breach notification laws.
- Most states, even those with comprehensive privacy regulations, have carve outs for certain types of entities including entities that may be regulated by other laws like HIPAA.

GUNSTER

Enforcement

- Just as the are a plethora of privacy laws there are numerous federal and state agencies enforcing these laws.
- Who are these regulators?
  - Federal Trade Commission (FTC)
  - HHS Office of Civil Rights
  - Securities and Exchange Commission
  - Consumer Financial Protection Bureau
  - Department of Justice
  - States
  - Others

GUNSTER

Enforcement Examples

- HIPAA – 4 Tier Penalty System based on level of culpability from reasonable to willful neglect. Penalties have annual cap of $1,500,000 with inflation related adjustments.
  - T1 – Unaware of violation and used reasonable due diligence.
  - T2 – Reasonable cause that entity should have known about the violations.
  - T3 – Willful neglect of HIPAA rules but corrected within 30 days of discovery.
  - T4 – Willful neglect of HIPAA rules but not corrected within 30 days of discovery.

GUNSTER

Enforcement Examples - HIPAA

- **Snooping in Medical Records by Hospital Security Guards Leads to $240,000 HIPAA Settlement**
- OCR has announced a settlement with Yakima Valley Memorial Hospital, a not-for-profit community hospital located in Yakima, Washington resolving an investigation under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. OCR investigated allegations of several security guards from Yakima Valley Memorial Hospital, who impermissibly accessed the medical records of 419 individuals. To voluntarily resolve this matter, Yakima Valley Memorial Hospital agreed to pay $240,000 and implement a plan to update its policies and procedures to safeguard protected health information and train its employees to prevent this type of snooping behavior in the future.

GUNSTER

Enforcement Examples - HIPAA

- **HHS Office for Civil Rights Reaches Agreement with Health Care Provider in New Jersey That Disclosed Patient Information in Response to Negative Online Reviews**
- OCR has announced a settlement with Manasa Health Center, LLC, a health care provider in New Jersey that provides adult and child psychiatric services. The settlement resolves a complaint received by OCR in April 2020, alleging that Manasa Health Center impermissibly disclosed the protected health information of a patient when the entity posted a response to the patient's negative online review. Following an OCR investigation, potential violations of the HIPAA Privacy Rule include impermissible disclosures of patient protected health information in response to negative online reviews, and failure to implement policies and procedures with respect to protected health information. Manasa Health Center paid $30,000 to OCR and agreed to implement a corrective action plan to resolve these potential violations.

GUNSTER

Enforcement Examples - HIPAA

- **HHS Office for Civil Rights Settles HIPAA Investigation with Arizona Hospital System Following Cybersecurity Hacking**
- **Banner Health pays $1.25 million to settle cybersecurity breach that affected nearly 3 million people**
- OCR has announced a settlement with Banner Health Affiliated Covered Entities ("Banner Health"), a nonprofit health system headquartered in Phoenix, Arizona, to resolve a data breach resulting from a hacking incident by a threat actor in 2016 which disclosed the protected health information of 2.81 million consumers. The potential violations specifically include: the lack of an analysis to determine risks and vulnerabilities to electronic protected health information across the organization, insufficient monitoring of its health information systems' activity to protect against a cyber-attack, failure to implement an authentication process to safeguard its electronic protected health information, and failure to have security measures in place to protect electronic protected health information from unauthorized access when it was being transmitted electronically. As a result, Banner Health paid $1,250,000 to OCR and agreed to implement a corrective action plan, which identifies steps Banner Health will take to resolve these potential violations of the HIPAA Security Rule and protect the security of electronic patient health information:

GUNSTER

Enforcement Examples - HIPAA

- **Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations**
- A U.S. Department of Health and Human Services Administrative Law Judge (ALJ) has ruled that The University of Texas MD Anderson Cancer Center (MD Anderson) violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and granted summary judgment to the Office for Civil Rights (OCR) on all issues, requiring MD Anderson to pay $4,348,000 in civil money penalties (CMPs) imposed by OCR.
- Not so fast…..
- University of Texas M.D. Anderson Cancer Center v. United States Dept. of Health and Human Services 985F.3d 472 (5th Cir 2021).

GUNSTER

Enforcement Examples - FTC

- FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising

  Under proposed order, GoodRx will pay a $1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data to Facebook, Google, and other companies

- Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges

  Epic will pay a $275 million penalty for violating children's privacy law, change default privacy settings, and pay $245 million in refunds for tricking users into making unwanted charges

GUNSTER

Enforcement Examples - FTC

- FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook

  FTC settlement imposes historic penalty, and significant requirements to boost accountability and transparency.

- FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads

  FTC and DOJ Order Twitter to Pay $150 Million Penalty for Violating 2011 FTC Order and Cease Profiting from Deceptively Collected Data

GUNSTER

Enforcement Examples - SEC

- SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies
  - Requires reporting of material cybersecurity incidents
- MGM 8-K 10/5/2023
- Caesars Entertainment 8-K 9/7/2023

GUNSTER

Enforcement Examples – States

- **AG Healey Joins Nationwide Settlement With Google Over Location Tracking Practices**
  - Attorney General Maura Healey today announced that she has joined a coalition of 40 attorneys general in reaching a $391.5 million settlement with Google for misleading consumers about its location tracking practices. This is the largest multistate data privacy settlement ever reached by attorneys general in the history of the United States. Massachusetts is expected to receive $9.3 million from the settlement.
- **AG James: Google And Youtube To Pay Record Figure For Illegally Tracking And Collecting Personal Information From Children**
  - New York Attorney General Letitia James today announced that Google, LLC (Google) and YouTube, LLC (YouTube) have agreed to pay a record $170 million in a national settlement, $34 million of which will go to New York State, for violating the Children's Online Privacy Protection Act (COPPA) by specifically tracking and serving targeted advertisements to users watching videos directed to children under the age of 13 on YouTube.

GUNSTER

Enforcement Examples – States

- Sephora, Inc., in a stipulated judgment, agreed to pay $1.2 million to resolve allegations that the company violated the California Consumer Privacy Act (CCPA). The Attorney General alleged that Sephora failed to disclose to consumers that it was selling their personal information, that it failed to process user requests to opt-out of sale via user-enabled global privacy controls in violation of the CCPA, and that it did not cure these violations within 30 days. The settlement requires Sephora to clarify its online disclosures and privacy policy; provide mechanisms for consumers to opt-out of the sale of personal information, including via the Global Privacy Control; conform its service provider agreements to the CCPA's requirements; and provide reports to the Attorney General.