Privacy Laws Governing Collection and Use of Customer Information

Boston University School of Law
Entrepreneurship and IP Clinic

Overview

- Defining personally identifiable information
- Discussing common privacy laws
- Reacting to a breach
- Best practices to follow

- High level overview - come talk to us!

What is Personally Identifiable Information?

- Many different definitions presented by different laws
  - Narrow definition
  - Broad definition
- Identify which laws impact your company in order to determine whether the information you are collecting is personally identifiable information

Examples

Massachusetts 93(h)

“Personal information” is a resident’s first name and last name or first initial and last name in combination with…

(a) Social security number
(b) Driver’s license or state ID card number
(c) Financial account number or debit/credit card number...

Health Information Portability & Accountability Act (HIPAA)

Protects “health information,” “individually identifiable health information,” and “protected health information.” Information protected includes, but is not limited to, healthcare records and related information that *could* be used to identify the individual.

Privacy Laws

Federal Privacy Laws

- Health Information Portability & Accountability Act (HIPAA)
  - Applies to types of health service providers
- Family Educational Rights and Privacy Act (FERPA)
  - Applies to schools that receive federal funding
- Children’s Online Privacy Protection Act (COPPA)
  - Applies to websites or apps that know that they are collecting information from children under the age of 13
- Gramm-Leach-Bliley Act (GLBA)
  - Applies to companies are involved in financial services

FTC Act Section 5

- “Unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful.”
- Unfair: could cause injury to customers
  - Wyndham Hotels
    - Credit card information was poorly stored resulting in multiple breaches
    - FTC determined that this disregard constituted unfair practices
- Deceptive: could defraud customers
  - Snapchat
    - Claimed images delete after a time, but this was false
    - Images were stored
    - FTC determined that this was a deceptive practice

Electronic Communications Privacy Act (ECPA)

- Wiretap Act
  - Regulates interception of communications
  - Campbell v. Facebook
    - Facebook scanned users' private messages
    - Court found that the users had not consented to Facebook reading their private messages
- Stored Communications Act
  - Regulates communications in storage and ISP subscriber records
- Pen Register Act
  - Regulates trace and trap devices and metadata
- These statutes do not apply when entities receive consent from consumers

Telephone Consumer Protection Act (TCPA)

- Restricts making of telemarketing calls, use of automatic telephone dialing systems and prerecorded voice messages
  - Also applies to companies that send text messages
- Companies must get consent from customers or follow strict solicitation rules
  - Must honor the National Do Not Call Registry

Computer Fraud and Abuse Act (CFAA)

- Prevents unauthorized access to computers
  - Prohibits scraping and hacking in some cases
- MBTA v. Anderson
  - The court found that a violation of the CFAA only occurs if the person knowingly causes the transmission of programmed information to a protected computer.
- Penalties include fines or imprisonment

MA Information Security Laws

- Must implement an information security program if have possession of personal information of MA residents
- Require that companies notify the State and affected residents when anyone acquires customers' personal data and there is a substantial risk of identity theft or fraud
    - PII is social security number, state ID, or financial account information

Reacting to a Breach

Do not delay in responding

- Yahoo Breach
  - Breaches occurred between 2013 and 2016
  - Yahoo initially reported that 1 billion accounts were affected; later admitted that 3 billion accounts were impacted
  - Yahoo took more than 3 years to reveal the first breach
  - Legal repercussions for this course of action
    - Several lawsuits
    - Investigation by Congress
    - Decreased its value in Verizon’s acquisition

Do not negotiate with the hackers

- Uber
  - Compromised sensitive information of millions of users and drivers
  - Breach occurred in October 2016
  - Chief Security Officer hid the breach
    - Paid hackers $100,000 to delete data and keep the breach a secret

Consider applicable law and scale of breach

- Applicable Law
  - 48 states currently have data breach notification laws
  - Additionally, there are federal laws that require notification (including HIPAA and GLBA)
- Scale of Breach
  - How quickly you are required to notify customers may be impacted by the size of the breach
  - Similarly, the method of notice required to be given to customers may be impacted by the size of the breach

Respect your customers

- Be candid about the breach
- Consider what a hacker could do with this information and give customers an opportunity to react appropriately
  - Ex. change passwords
  - Ex. credit monitoring

Best Practices

Adopt some level of protection for customers

- Be honest
- Strive to keep your customers safe
- Do not over-represent your practices - only guarantee what you can guarantee
    - Ex. Do not guarantee anonymity

Do not copy/paste privacy policies

- Privacy policies are not a one-size-fits-all solution
  - Applicable laws can vary by state and the type of information collected
  - For example, CalOPPA is the only state law that requires a privacy policy
- Your privacy policy needs to be tailored to the type of information you are collecting from customers
  - For example, if you are collecting information from children under age 13, COPPA is triggered
- Retain counsel to assist with the drafting of a privacy policy

Think about what laws apply to your company

- If you work with healthcare information, consider HIPAA
- If you work in the financial space, consider GLBA
- If you work with children, consider COPPA
- If you work in education, consider FERPA

Consider the information you have

- How could this information be misused if it fell into the wrong hands?
- How can you prevent these uses from occurring?

Have a plan in case of inadvertent disclosure

- Know what laws apply in case data has been impermissibly disclosed
- Know what the relevant laws require you to do in the event of such a disclosure
- Have a checklist of what these laws require so that you are able to react to an impermissible disclosure quickly

To learn more about the Entrepreneurship and IP Clinic and its services, visit sites.bu.edu/elawclinic

To learn more about the Technology and Cyberlaw Clinic and its services, visit https://sites.bu.edu/tclc/