It’s not just your data: your company’s obligations to protect customer data

Rachel Marmor, Counsel, New York City

DWT.COM

Davis Wright Tremaine LLP

Why Worry?

Regulatory Risk

- FTC Act and state UDAP laws require data uses to be fair and transparent
- Laws require companies to publish a privacy policy on their websites; app stores require same
- Laws require reasonable security

Financial Risk

- Costs of a security breach could bankrupt a small business
- Potential loss of revenue due to privacy or security incident
- M&A process includes privacy and security diligence

Reputation Risk

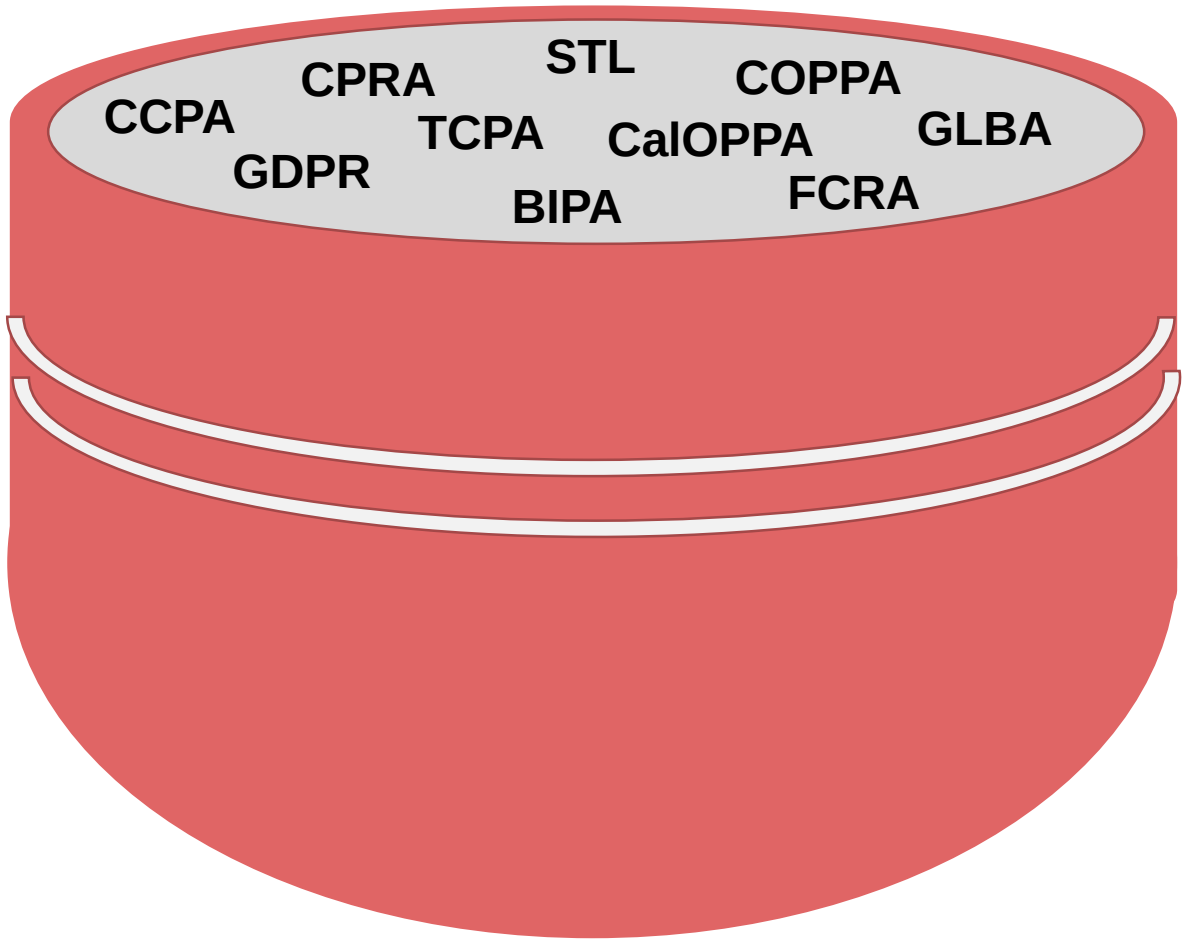
- Privacy missteps create great headlines
- Customers may make choices based on a business's perceived reputation for handling privacy and security

What is “Personal Information”?

Any information that can “reasonably” be linked to a particular person or device.

Includes persistent identifiers such as customer numbers, Device ID, MAC Address, and IP address.

Alphabet Soup of Privacy Laws



What can I do with customer data?

- Generally, any internal uses you want, ***but***:
  - The collection and use needs to be disclosed to the customer
  - New collections or new uses require additional notice
  - Sensitive data should only be collected when necessary to achieve a business purpose, and transparency is necessary
- Few restrictions on use for first-party marketing
- Sharing of data with service providers is fine. Sharing of data with other third parties could be subject to an opt-out right.

High Risk Customer Data

- Payment card information
- SSN, driver’s license, state identification card, or passport number
- Financial account info
- Health information
- Precise geographic location
- Biometric information
- Information about race, ethnicity, sexual orientation, political/religious opinion, trade union membership
- Data about minors under 13

Privacy Policy Requirements

- The Privacy Policy must disclose:
  - What personal information you collect, including information collected by cookies
  - The purposes for which that information is used
  - The circumstances in which that information is disclosed to an external party
  - Individuals' options and rights with regard to their personal information
  - Contact information for privacy questions
  - Last updated date
- Additional disclosures may be required if CCPA, GDPR, Nevada law, COPPA, etc. apply

Common Privacy Policy Mistakes

- “By continuing to use our website, you agree to the terms of this Privacy Policy.”
- “The information we collect is anonymous.” / “Non-personal Information” / “Anonymous cookie”
- “We do not sell or rent your information.”
- Use of term “third party service provider.”
- “Except as disclosed in this Privacy Policy, we do not share your information.”

Sharing Customer Information

- Companies frequently leverage “service providers” for tasks such as cloud hosting, website hosting, and website analytics. Such contracts ***should*** contain clauses restricting the service provider from using the PI other than to provide the service.
  - Required under CA law and GDPR; best practice otherwise.
  - Contracts should also provide for disposal of data when no longer necessary.
- You remain responsible for the security of PI when you allow service providers to host or access it.
- Sharing of data with a party who is not restricted in its use may require an opt-out.

Protecting Customer Data

- FTC Guidance:
  1. Start with security
  2. Control access to data sensibly
  3. Require secure passwords and authentication
  4. Store sensitive personal information securely and protect it during transmission.
  5. Segment your network and monitor who’s trying to get in and out.
  6. Secure remote access to your network.
  7. Apply sound security practices when developing new products.
  8. Make sure your service providers implement reasonable security measures.
  9. Put procedures in place to keep your security current and address vulnerabilities that may arise.
  10. Secure paper, physical media, and devices.

Questions