

Software Copyright and Fair Use

- **Computerized records = new privacy threats:** unknown databases have your info, one-to-many dissemination, collection of different types of info
- **Fair Information Principles:**
 - **Notice:** A person should be provided notice of what an organization of computer system is collecting, using, and sharing regarding their data; WHY? value of transparency, commitment to promises
 - **Appropriate Uses:** A person's information should be used for "appropriate" purposes
Primary uses: what was info collected for, Secondary uses: national security, public health and safety, law enforcement purposes
 - **Individual Choice:** Gives data subject some control over their information, Opt-In/Opt-out programming
 - **Access and Correlation:** Calls on organizations collecting information to provide individual access, A person should be able to know what information about them is being held in the system, A person should be able to use a process to change any incorrect information in that database
 - **Security:** Information cannot be kept private if it is not held securely, Reasonable administrative, process, technical safeguards to protect the data
 - **Other Fair Information Practices:** Minimization, Downstream assurances, Mitigation of privacy harm that occurs, Data breach notification
- **HIPAA:** Only health information covered by certain kinds of organizations. Excluded: Free services, Those using paper records, Many mobile apps (not providers, plans, or healthcare clearinghouses)
- **Breach Notification Laws:** In 2003, California enacted a law requiring companies to notify any California resident whose computerized data was breached •Today, every state has a data breach notification law. HIPAA also was amended to add a data breach notification provision
- **What Data Triggers Notification:** Name, SSN, DL number, Account/credit card info, sometimes: medical data, student data, biometrics
- **EXAMPLE Equifax Data Breach:** slow to react, communicated wrong information, set up unsecure second website, tried to profit from credit-free solutions offered to those effected
- **Section 5 of FTC:** Provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful".
- **General Data Privacy Regulation:** Notice (Access with rectification (Correction)), Lawful Basis for Processing (Consent and appropriate use: contractual necessity, legitimate interests of organization. "Right to Be Forgotten" (Data subject can request the erasure of information about them, Exceptions: Freedom of expression, necessary for health/science purposes)

CRPA Compliance and Automated Compliance Checking

- Went into effect in Jan 2020, consists of 6 important privacy rights, including right to opt-out of sale of personal information
- Any for-profit business in Cali that has >\$25 million annual gross, >\$50% of revenue selling consumer personal data

RQ3:
Do the businesses that implement the opt-out link also let non-Californian consumers opt-out?

453 (78%) websites implement the opt-out link in CA also implement across all states.

CA	VA	CO	UT	IL	# websites
✓	✓	✓	✓	✓	453
✓	✓	✓	✓		13
✓	✓	✓		✓	6
✓	✓	✓			25
✓	✓		✓		6
✓	✓				55
✓					9
Other combinations of states					14



Summary

- **RQ1:** How does the implementation of the CCPA's opt-out requirements change over time?
- **RQ2:** Are websites complying with the CCPA opt-out requirements?
- **RQ3:** Do the businesses that implement the opt-out link for the sale and sharing of personal data also let non-Californian consumers opt-out?
- **RQ4:** Do businesses that fail to provide opt-out links on their home page offer other opt-out methods, or are they not subjected to CCPA?

Websites are increasingly but not fully complying with CCPA's requirements.

45% fail to meet requirements for appearance of opt-out

453 (78%) websites implement the opt-out link in CA also implement across all states

147 (30%) websites that are likely subject to CCPA still do not implement the opt-out link.

Reasons for failure to comply to the CCPA are varied and ambiguous.

- Opt Out Methods:
 - Before CPRA: Do Not Sell My Personal Information, After CPRA: Do Not Sell or Share My Personal Information, Your Privacy Choices, Frictionless opt-out preference signals (GPC)

Censorship

Taxonomy of Modern Censorship

- Fear: make people afraid to publish or view content
 - Threats, prison, ex. Journalists ; consequences and banning
- Friction: make it difficult to find or access content
 - Technical Measures: porous firewalls, throttling (slowing down performance), manipulation (search results etc.), local versions of sites
 - Great Firewall is a porous firewall, chinese government slowing google speeds (throttling)
- Flooding: dilute the discours w irrelevant/distraction info
 - Bots post distracting info, propaganda and misinformation

Technical implementation of Censorship

- Protocol interference and manipulation: IP filtering (VPNs can circumvent), DNS manipulation and poisoning, TCP connection resets, HTTP(s) redirection
- Infrastructure interference: DNS registries, Certificate authorities, Content delivery Networks (CDNs)
- Platform interference: Social Media and search engines
- Legal and policy based:
 - Communications Decency Act (Section 230): prohibited treating online service providers as the publisher or speaker of content provided by others or holding providers liable for attempts to eliminate objectionable content
 - Digital Millennium Copyright Act (Section 512): limitations on liability—referred to as safe harbors— for four types of online service providers. The safe harbors shield qualifying online service providers from monetary liability for copyright infringement based on the actions of their users, in exchange for cooperating with copyright owners to expeditiously remove infringing content and meeting certain conditions.

Types of Censorship (China Specific)

1. Great Firewall: disallows entire sites from operating in the country
2. Keyword Blocking: blocks users from posting banned words or phrases
 - a. Possible to evade, Citizens using homophones
3. Online censors that specifically remove posts

VPNs

- Encrypt and tunnel user's traffic through proxy server. Hides IP address, location
- Doesnt hide device info, stop cookies or tracking scripts,
- VPN provider can still view your data by collecting the VPN logs. This is just a shift of trust to your VPN provider