* “The U.S. Privacy Act (1974) articulates six principles including: ensuring an individual can determine what data is collected; guarantee that data collected is only used for the purpose for which it is collected; provides access to your own data; and the information is current, correct and only used for legal purposes [1]. The Act provides explicit clauses to collect damages if privacy is violated but it also permits explicit statutory exemption if there is an important public policy need. The Organisation for Economic Cooperation and Development (OECD) have developed a list of eight principles including: limited collection, data quality assurance, purpose specification, limited use, security safeguards, openness, individual participation and accountability to guide providers and collectors to undertake best practices”

# Children's Online Privacy Protection Rule ("COPPA")-

* Not a lot of federal law regarding internet privacy. Like with many issues, the federal government leaves a lot of the details up to each state. Laws also differ depending on the industry, which results in a confusing mess of rules and regulations for US website owners to navigate.

The FTC (Federal Trade Commission) regulates business privacy laws. They don't require privacy policies per se, but they do prohibit deceptive practices.

Some federal laws that touch on data privacy include the Health Insurance Portability and Accountability [**Act of 1996**](http://www.hhs.gov/ocr/privacy/) (HIPPA), which deals with health-related information, and the Children's Online Privacy Protection Rule ([**COPPA**](https://www.privacypolicies.com/blog/coppa/)), which applies to websites that collect data from children under the age of 13. Some states have more stringent laws than others, such as the California Online Privacy Protection Act ([**CalOPPA**](https://www.privacypolicies.com/blog/caloppa/)), which is the first law in the United States that specifically requires websites to post a Privacy Policy.

CalOPPA actually applies not just to websites based in California, but to any website that collects personal data from consumers who reside in California. With that in mind, website owners based in the United States are encouraged to err on the side of caution so they don't run into legal trouble inadvertently.

CalOPPA requires that every website that collects personal data from users post a privacy policy that includes:

* The type of personal data collected
* Any third parties you share the data with
* How users can review and change their data that you've collected
* How you'll update users of changes to your Privacy Policy
* Your Privacy Policy's effective date
* How you'll respond to Do Not Track requests

If there's any chance that you'll be collecting personal data from anyone in California, it's best to comply with this law by creating an accurate privacy policy.

A few additional laws to be aware of in the US include the [**California Consumer Privacy Act**](https://www.privacypolicies.com/blog/california-consumer-privacy-act/) (CCPA) and the [**Washington Privacy Act**](https://www.privacypolicies.com/blog/wpa-v-ccpa/) (WPA)

* + **Laws regarding our Scope**
    - According to the US Cyberbullying law is it illegal to create a fake account that is intended to impersonate someone with malicious intent/harass someone/illicit illegal activity
      * However, in the case of our project, we would be making fake accounts but we are not impersonating someone/harassing anyone else. If we did anything with the account that was targeted towards another individual human we may run into an issue but as of right now we look in the clear. This is a grey area but my opinion is that we are ok
      * Computer Fraud and Abuse Act (CFAA)
        + Doesn’t apply to us in this scenario as it focuses more on hacking not making/lying about account information
      * Financial Transactions (Like bank accounts) need to be real names and for other financial transactions fake names are fine as long as we do not get financial gain from using the name