**Policy statements that could be quantifying values**

* Ability to accurately access all the information that a company has on a specific user
  + Furthermore, how easy for this to happen? (Walmart refers to third party, google shows you info)
* Purpose, Visibility, Granularity, and Retention
* 3rd party
  + use /transfer/ restrict information to a 3rd party
    - Lack of responsibility to an affiliate (data/legal shield)

(using violation fine amount as a reference point/quantifying value)

**(Notes on Privacy Policy Language)**

* While some privacy policy seems straightforward some of the privacy protections that are claimed were not honored. Which makes it difficult to quantify based on specific language.
  + Even when consent is not given, cookies will be used to exploit users to be shown more relevant ad information.
* Reading the California compliant information helps to get a clearer picture of consumer rights
* Quantifying Privacy Violations (GREAT STARTING POINT FOR THIS)
  + Mishtu Banerjee, Rosa Karimi Adl, Leanne Wu, and Ken Barker
    - “The taxonomy represents privacy as a point in a four-dimensional space, where each dimension represents a diﬀerent privacy predicate: **purpose, visibility, granularity and retention**. Purpose refers to the uses for which data has been collected. Visibility describes the parties who will have access to the data while it is in storage. Granularity deﬁnes the speciﬁcity of data which will be revealed. Retention describes how long the data will be kept in storage.”
      * Purpose- information stored only for a specific purpose and only for that purpose/ does not continue after the purpose is completed
        + A lot of internet vendors have weak visibility
    - “The essential idea we are building up to is that a privacy violation occurs when the privacy policy of a house exceeds the privacy preferences for a data provider around a speciﬁc datum the data provider supplies.”
    - “The taxonomy, therefore, deﬁnes three kinds of ‘players’ in a data privacy scenario. There are data providers who provide raw data. There is the house, which is the organization that maintains a data repository. This is generally the party that stands to proﬁt from any use of the data, regardless of whether the data provider’s privacy has been protected. There are also third-parties who have access to the data maintained by the house. The interactions of these players constitute a privacy gamble, in which data providers exchange their data in return for services, and risk having their privacy violated by the house or third-parties. “
* “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”
  + A Data Privacy Taxonomy
    - COPPA
      * “Children’s Online Privacy Protection Act, to clarify the scope of the Rule and strengthen its protections for children’s personal information, in light of changes in online technology since the Rule went into effect in April 2000”
      * This is where the Age 13 limit comes from and how companies gather large fines if collecting information on someone younger than 13
        + <https://www.ftc.gov/system/files/2012-31341.pdf>
* We could potentially focus on pursuing pre-existing legislation such as the GDPR and the CCPA, to more clearly define privacy expectations, and compare coverage differences between them and not having any sort of privacy protection.
* Since one must be a resident of California to benefit from the CCPA (and some sites verify users’ geolocation based on IP address), after allocating a portion of the fake IDs to claim to be CA residents, we could use a VPN to spoof their geo-location data while browsing to maintain eligibility. The same process could be used for GDPR eligibility.
  + Josh