Catalog of Problematic Data Actions and Problems

This catalog is a *non-exhaustive*, *illustrative* set of problematic data actions and problems that individuals could experience as the result of data processing or their interactions with systems, products, or services.

# Problematic Data Actions

**Appropriation:** Data is used in ways that exceed an individual’s expectation or authorization (e.g., implicit or explicit). Appropriation includes scenarios in which the individual would have expected additional value for the use given more complete information or negotiating power. Privacy problems that appropriation can lead to include loss of trust, loss of autonomy, and economic loss.

**Distortion:** Inaccurate or misleadingly incomplete data is used or disseminated. Distortion can present users in an inaccurate, unflattering, or disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty.

**Induced Disclosure:** Induced disclosure can occur when individuals feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or rights to an essential (or perceived essential) service. It can lead to problems such as discrimination, loss of trust, or loss of autonomy.

**Insecurity:** Lapses in data security can result in various problems, including loss of trust, exposure to economic loss and other identity theft-related harms, and dignity losses.

**Re-identification:** De-identified data, or data otherwise disassociated from specific individuals, becomes identifiable or associated with specific individuals again. It can lead to problems such as discrimination, loss of trust, or dignity losses.

## Stigmatization: Data is linked to an actual identity in such a way as to create a stigma that can cause dignity losses or discrimination. For example, transactional or behavioral data such as the accessing of certain services (e.g., food stamps or unemployment benefits) or locations (e.g., health care providers) may create inferences about individuals that can cause dignity losses or discrimination.

**Surveillance:** Data, devices or individuals are tracked or monitored in a manner disproportionate to the purpose. The difference between a benign action and the problematic data action of surveillance can be narrow. Tracking or monitoring may be conducted for operational purposes such as cybersecurity or to provide better services, but it can become surveillance when it leads to problems such as discrimination; loss of trust, autonomy, or liberty; or physical harm.

**Unanticipated Revelation:** Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to dignity losses, discrimination, and loss of trust and autonomy.

**Unwarranted Restriction:** Unwarranted restriction includes not only blocking access to data or services, but also limiting awareness of the existence of data or its uses in ways that are disproportionate to operational purposes. Operational purposes may include fraud detection or other compliance processes. When individuals do not know what data an entity has or can make use of, they do not have the opportunity to participate in decision-making. Unwarranted restriction also diminishes accountability as to whether the data is appropriate for the entity to possess or it will be used in a fair or equitable manner. Lack of access to data or services can lead to problems in the loss of self-determination category, loss of trust, and economic harm.

# Problems

**Dignity Loss:** Includes embarrassment and emotional distress.

**Discrimination:** Unfair or unethical differential treatment of individuals whether singly or as a group arising from the processing of data.

**Economic Loss:** Can include direct financial losses as the result of identity theft or the failure to receive fair value in a transaction.

## Loss of Self Determination

* **Loss of Autonomy:** Includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement.
* **Loss of Liberty:** Incomplete or inaccurate data can lead to improper exposure to arrest or detainment. Improper exposure or use of information can contribute to abuses of governmental power.
* **Physical Harm:** Physical harm or death.

**Loss of Trust:** The breach of implicit or explicit expectations or agreements about the processing of data. These breaches can diminish morale or leave individuals reluctant to engage in further transactions potentially creating larger economic or civic consequences.