

Designing a Coordination Mechanism for Managing Privacy as a Common-Pool Resource

Challenge

- Automated collection and aggregation of personal data is a pervasive aspect of physical and digital infrastructure.
- Aggregation enables beneficial system functionality but it also produces potentially invasive insights and inferences.
- Users cannot currently coordinate about which uses of derived data are acceptable, such as those that make the system perform better, and those that are unacceptable, like making sensitive inferences that are unrelated to system operation.

Approach

- Derived data exhibits characteristics of a social dilemma:
 - It is an important aspect of the system's desirable functionality.
 - But, it also puts users at risk for inferences that could have negative consequences.
- Conceptualizing privacy this way shifts our thinking from personal preference and individual choice, to managing a shared resource by coordination and negotiation about what people should or shouldn't know about others.



derived data: *new inferences that cannot be directly collected from the environment by the sensors themselves*

Scientific Impact

- Semi-structured interviews will identify norms for acceptable uses of derived data, and experiments involving simulated norms violation and responses will validate those norms.
- Building on frameworks for analyzing social-ecological common pool resource systems, the project will iteratively design, prototype, and evaluate a privacy coordination mechanism for “smart home” systems that will support collective privacy management decisions.

Broader Impact

- This project addresses a problem with broad social importance: as “smart” devices with embedded sensors become more common, privacy in ubiquitous computing systems will increasingly be an issue that nearly everyone will encounter.
- Demonstrating that derived data can be collectively managed like a common pool resource will point to new kinds of solutions for digital privacy issues, and the outcomes of this project have the potential to shape discussions about policy and regulation.