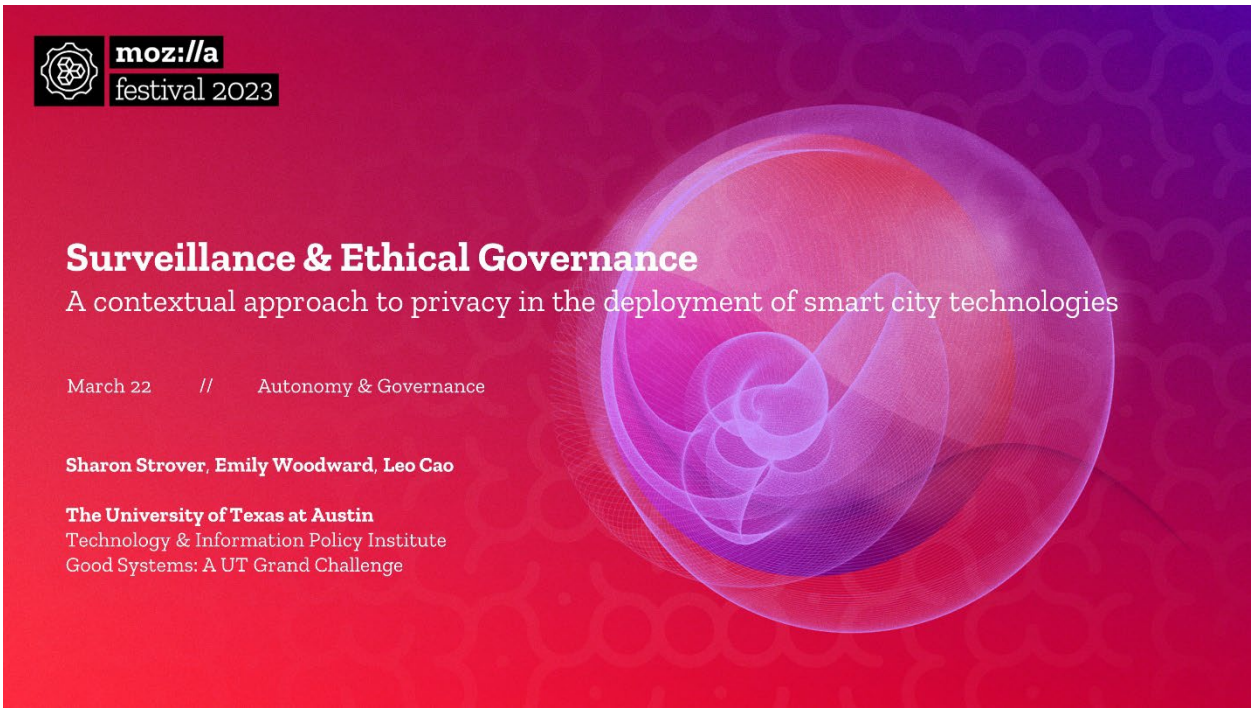

This case studies series is part of the research project Being Watched: Embedding Ethics in Public Cameras supported by Good Systems: A UT Grand Challenge. Two workshops that utilized the case studies materials have been presented by the TIPI team at ICEGOV 2022 and MozFest 2023. The vignette format was inspired by the AI and Ethics Case Studies at Princeton University.

Background

Many cities around the world are increasingly turning to AI-based surveillance technologies to achieve a variety of public benefits, raising important questions regarding privacy, accountability, and ethical governance.

- From CCTV cameras to environmental sensing systems, what does the use of smart technologies in urban environments entail?
- How does the adoption of such technologies complicate our conceptualization of privacy?
- How can we encourage meaningful public engagement and embed justice and accountability into these systems often criticized for their opacity?

Given the context-specific nature of privacy as a social value and informed by the Helen Nissenbaum's concept of contextual integrity, we have devised three fictional vignettes based on a series of actual events and ask readers to reflect upon a series of ethical issues regarding the use of surveillance technologies in the urban environment.

Objectives

- Illuminate the multiple aspects of surveillance technologies and privacy.
- Foreground the ethical issues surrounding the use of surveillance technologies.
- Explore contextual differences when deploying surveillance systems and managing the data they generate.
- Highlight public engagement strategies to establish good practices.
- Brainstorm ways to safeguard privacy while using surveillance systems for social benefits.

Instructions

We encourage readers to annotate the paragraphs or take notes as they read along and use the following questions to guide their reading and discussion of the three cases.

Case

- What is the problem in this case?
- What solutions do the stakeholders come up with?

Risk

- What are the potential risks of using technologies introduced in the case?
- Are there communities that may be disproportionately affected?

Accountability

- Are there regulatory measures that ensure government accountability?
- How are partnerships with technology companies managed?

Trust

- How are local communities brought into the decision-making process?
- What actions should/could citizens take to voice their concerns?

#01 Security Cameras at Local Businesses

In the city of Midway, local government council members have been receiving complaints from business owners about theft and property damage that took place in one of the city's central business districts. After an internal discussion, the city council announced a plan that would require all local businesses in certain districts to install security cameras outside the premises and encourage business owners to optionally install cameras indoors as well. All cameras would be clearly visible and marked with signage. Real-time video footage would be accessed and monitored by the Midway Police Department (MPD). A local tech entrepreneur offered to purchase and donate all required cameras to the city, while the cost of installing and maintaining the system would be split between the local government and the business owners according to a partnership agreement drafted by MPD.

In the following six weeks, the city held a number of public engagement sessions, informing business owners and local residents about the proposed plan, explaining the rationale behind the decisions, and trying to address some of the concerns community members might have. Due to overwhelming pushback from civil rights groups regarding the use of facial recognition technology, the city council decided not to incorporate facial recognition capabilities in these camera systems.

Eight months later, an international hacktivist group hacked and released a massive amount of government data in several countries. Included in this hack were data from Midway's local cameras, stored in a regional fusion center, to which the city of Midway is connected. These government-owned fusion centers aggregate and analyze data collected by local police and other departments from all cities in the region to assist law enforcement and national security. Despite the promise of MPD not to use facial recognition in the city, these fusion centers did utilize a wide array of data processing techniques, including facial recognition and biometric identification. In response to the release of hacked data, MPD explained that they do not have jurisdiction over regional fusion centers and suggested that information provided by the fusion center had in fact helped solve several high-profile violent crimes in the city. Nonetheless, many business owners have requested to withdraw from the camera network, and some council members have also suggested an overhaul of the program, citing eroding trust among an increasing number of local residents and community groups.

#02 Environmental Sensing Network on Streetlights

The city of Citrusville has long suffered from sandstorms due to its geographic location. The local government has been trying to implement technological solutions to combat this natural disaster and mitigate its public health impact, especially in terms of building an environmental monitoring and warning system. Inspired by the concept of the 'smart city,' Citrusville wanted to build a smart sensing network into the city's existing physical infrastructure. Eventually, the city's transportation and utilities departments as well as the chief information officer established a collaborative initiative to retrofit the city's streetlight network with a smart sensing system capable of monitoring air quality and collecting other environmental data. The system will also be equipped with cameras that monitor traffic data in order to improve road safety and emergency response. Most importantly, the initiative promises to pay for itself by installing energy efficient light bulbs that reduce the city's energy bill in the long run.

One year later, the initiative was widely considered a success and expanded from a pilot project to cover the entire city. However, a local investigative journalist recently revealed that the Citrusville Police Department (CPD) had "tapped into" the sensing network by adding additional com-ponents to the streetlight modules, such as "shot spotters" and automat-ed license plate readers. They did this without informing the public or the city council. CPD justified its action by arguing that all the surveillance technologies added to the streetlight network had already been approved by the city council and their use therefore complied with the city's existing Surveillance Technology Code of Practice. Disclosing where every piece of surveillance technology is installed, according to CPD, would be impractical and counterproductive to fighting crime.

Following the media exposé, the company originally contracted to manufacture the streetlight module considered the unauthorized addition of surveillance technologies to its product not only a breach of contract on the part of the city but also a damage to the company's reputation for respecting user privacy. The company soon threatened to terminate the partnership and sue the city. The mayor and city council both agreed that the surveillance components of the network be disabled, but the module was built in such an interconnected way that it could not be selectively shut down without affecting the lighting grid of the entire city.

#03 Dash Cam Footage on Bike-Sharing System

Coast City is an international hub of technology startups and home to one of the nation's largest electric bike manufacturers, Bykr, which has an extensive e-bike rental and share network in the city. One year ago, Bykr started to collaborate with the city government on a new project that will equip all its e-bikes and charging stations with a module that includes a dash camera, a LiDAR (light detection and ranging) sensor, and a set of environmental sensors to detect temperature, humidity, pressure, and air quality. Bykr hopes to use data collected by the LiDAR sensors to launch its map services and self-driving vehicle division. In return for the city's support, Bykr promised to release all the environmental data in an open access format through an API that is free of charge to the public. To protect user privacy, Bykr specifies in its Terms of Service that video footage recorded by the bike-mounted dash cameras is encrypted by default. Users can review and save a copy of the video within 24 hours after the ride, after which the footage will be deleted automatically.

Last month, an armed robbery resulting in three deaths took place at a store near a Bykr charging station. The Coast City Police Department (CCPD) reached out to Bykr with a court-issued warrant that requested footage recorded by the camera installed at the charging station as well as those recorded by bike-mounted cameras on bikes that were in the vicinity of the crime scene before and after the robbery took place. Bykr provided the station footage but claimed that they were unable to provide most bike footage unless users had turned off the default data encryption. Bykr also declined CCPD's request for the company to decrypt the footage on the grounds that it would violate its own terms of service and the company's belief in protecting user privacy.

In the meantime, Bykr has been using data collected by the LiDAR sensors to improve its map services and develop new self-driving technologies. However, due to the ongoing confrontation with CCPD on whether to decrypt video footage, the city has refused to renew a permit that allows companies to provide self-driving rides in some parts of the city. Negotiations between Bykr and the city are underway, but for now the company has suspended public access to its API that gives access to environmental data collected by the bike network.