Stanford
University Privacy Office

GUIDING PRINCIPLES FOR THE USE OF SENSORS ON CAMPUS

Background

We expect that sensors – electronic devices that detect and respond to stimuli – will become increasingly pervasive in our daily lives, as they continue to become smaller, less expensive, and more powerful. This will drive a proliferation of databases containing vast amounts of personal information, which in turn can be combined with other databases globally and across industries.

In many contexts, sensors collect non-personal information about objects or environmental conditions. For example, in cities, factories and agricultural fields, sensors collect data to reduce traffic, manage energy consumption, and measure soil and water quality – all without the need to identify individuals. In other contexts, however, sensors may collect personally identifiable information. For example, facial recognition and other biometric sensors can be used to identify and monitor individuals in the interests of safety and security; and most smartphones have an accelerometer, gyroscope, GPS and a variety of other sensors that provide detailed information (such as real-time location) about the device and thus the person holding it.

To be sure, sensor technology offers the potential for unprecedented social, health and economic benefits. But to the extent that personal information is collected and processed on a massive scale, substantial privacy and ethical concerns may arise. Anonymity may be difficult or impossible when surrounded by sensors; and autonomy and fundamental human rights may be negatively affected.

In light of current trends, the University Privacy Office (UPO) expects to receive a variety of requests to use sensors on campus, to share sensor data with third parties, and to combine data from Stanford-managed sensors with external datasets.

This document sets forth UPO's guiding principles when reviewing proposals regarding the deployment of sensors on Stanford property that collect personal information of Stanford students, faculty, staff and visitors, and the related processing of such information by Stanford or third parties.

Guiding Principles

UPO advocates for the innovative and ethical use of data, and believes that emerging technologies must be developed and deployed on campus in ways that respect the privacy of individuals. UPO supports the use of sensors on campus only in circumstances where the collection and processing of personal information is fair, transparent and accountable, and provides meaningful benefits to the Stanford community.

Below are guiding principles that UPO will reference when evaluating a proposed use of sensors on campus that collect personal information:

- Personal information should be processed fairly, ethically, lawfully and in a transparent manner.
- Individuals should be timely notified about the collection, use, transfer and retention of their personal information, in clear and simple language. The stated purposes should be specific; and any subsequent secondary or derivative use (including combination with another dataset for

such subsequent use) should require a separate notice and consent of individuals, pursuant to a separate data privacy risk assessment.

- Individuals should be timely given appropriate choices about the collection, disclosure, and use of their personal information, including where appropriate an opportunity to decline to provide personal information.
- Individuals should be given appropriate access to and ability to delete their personal information, subject to reasonable limitations.
- Individuals should be informed of any third parties that may access their personal information, and how their personal information may be combined with third party datasets.
- Only the minimum, relevant information necessary to accomplish the stated purposes of processing should be collected or processed.
- Sensors should collect or process sensitive personal information only when directly related to a specific service or benefit that an individual has affirmatively requested. Sensitive personal information includes biometric information (including face prints), precise geolocation, health information, information of children under 13, audio or video recordings, and contents of or identifiable parties to communications.
- Personal information should be kept complete, accurate and up-to-date, as reasonably necessary for the purposes for which it is processed.
- Reasonable and appropriate technical and administrative controls should be implemented to safeguard personal information against accidental or unauthorized loss, alteration, disclosure, use or access.
- Personal information should be promptly deleted or de-identified when no longer necessary to accomplish the original, stated purposes of processing.

The above principles are intended to apply in addition to all applicable law and Stanford policies and standards.*

Stanford faculty, staff and students can submit any questions or comments to UPO at https://privacyrequest.stanford.edu/.

• • •

*For example, without limitation: Completion of a Data Risk Assessment (https://uit.stanford.edu/security/dra), where Stanford's Minimum Security Standards (minsec.stanford.edu) and Minimum Privacy Standards (minpriv.stanford.edu) apply, is required before collection or use of High Risk data (https://uit.stanford.edu/guide/riskclassifications). In addition, the Stanford University Video Surveillance System Guidelines discuss requirements for video surveillance, monitoring and recording applications and installations deployed on campus for the purposes of safety and security (https://police.stanford.edu/pdf/vssguidelines.pdf). Use of drones with sensors must comply with Stanford's policy on Operation of Unmanned Flying Vehicles (https://doresearch.stanford.edu/policies/research-policy-handbook/environmental-health-and-safety/operation-unmanned-flying-vehicles).