



EGO4D's approach to privacy and ethics in data collection and release

Privacy and Ethics:

From the onset, privacy and ethics standards were critical to EGO4D. While necessary for any video collection, the first-person, daily-life nature of this initiative accentuates such considerations. EGO4D is also multi-modal, with some footage collected with additional paired data of audio recording, 3D environment scans, Inertial Measurement Unit (IMU) and eye tracking. EGO4D leveraged advanced de-identification processes and hours of human labor. This document summarises the overall approach of the consortium to privacy and data ethics.

EGO4D Standards:

With such a diverse consortium of institutions, from different countries, the approaches of each university to address privacy and research ethics issues naturally differ slightly. However, each group prioritized privacy and ethical data collection to the highest degree, with the following consortium standards ensured by each EGO4D partner:

- **Independent review and approval:** Prior to any data collection, all universities/organizations documented their study protocol, approaches to privacy and de-identification and participant consent standards. These protocols were reviewed by their institutional review boards or independent ethics committees against standards for research ethics, privacy, and informed consent. Ethics committee or IRB approval of each EGO4D study design was required before any data was collected or integrated into the dataset or research agenda.
- **Participant Consent:** Prior to contributing to EGO4D, all camera-wearers were informed about the purpose of the study and were given the opportunity to ask any questions of the research teams. All camera-wearers could withdraw at any point in time without giving justification. Consent forms or video release forms were signed and each university/organization maintains the record of all consent/release forms for acquired data.
- **Participant Control:** All camera-wearers personally selected activities that they would capture from a predefined list of daily activities. Participant control of data collection allowed autonomy in what scenes or activities were captured in their footage. Participants had the opportunity to

review videos to be released and delete all or parts of them¹. Particularly for indoor recording, subjects were explicitly instructed to when possible avoid collecting personal identifying data of themselves and others including faces, conversations, tattoos, jewelry, etc. This greatly reduced de-identification needs, making the process more robust and respectful of the subjects and bystanders' privacy. However, the responsibility of de-identifying any data lies with the researchers rather than the participants. The de-identification processes for EGO4D are detailed next.

- **De-identification:** Videos were de-identified, removing personally identifiable information, including, for example, blurring bystanders' faces or passing license plate numbers. Similarly, audio was removed from many videos for additional protection. In certain cases, study participants consented to have their likeness appear unredacted in the video and therefore were not de-identified or removed. In these cases, participants were fully informed of all permitted uses for EGO4D data and clearly consented to include their identifiable information in support of the advancement of AI for egocentric perception. In cases where this consent was not possible or was not obtained, videos were de-identified.

De-identification:

The EGO4D university consortium members undertook a comprehensive three-step de-identification process, deploying advanced video redaction software, open source tools, and hours of human reviews to ensure that identifiers present in the dataset without consent or other permission are de-identified. While each university's approach differed slightly, we followed these core approaches:

Step 1: Human Review of all Video Files:

In Step 1, all video from EGO4D was reviewed by an approved member of the university or institute to identify and assess potential privacy concerns. As part of this process, in certain cases, camera-wearers themselves reviewed their footage to flag any concerns to an approved member of the EGO4D research team they were collaborating with. As part of this Step 1 human review, de-identification requirements were scoped.

Step 2: Automated Reviews:

In Step 2, marked EGO4D videos were processed through de-identification software that removes specific identifiers at scale. EGO4D partners worked closely with leading commercial providers of video redaction software to leverage advanced tools to protect identities. We were specifically pleased to collaborate with [brighther.ai](#) and [SecureRedact](#). Technicians from these firms customized solutions to the specificities of first-person video and guided EGO4D universities through the de-identification process, working to deploy the software at scale.

Step 3: Human Review of Automated Blurring

While automated redaction software is a powerful tool to protect privacy, the best results combine these resources with human screening of outputs. EGO4D researchers carefully reviewed all outputs from automated blurring, identifying both instances of false positives (blurring that mistakenly occurred on non-privacy related items) or false negatives (inaccurate or

¹ University approaches varied between asking participant to review all the data after recording or inviting the participants to request the videos to review

insufficient automated blurring). As part of this process, approved members of each university or institute re-watched all video passed through the de-identification tools and engaged manual blurring or blur corrections. For this part of our de-identification process, we used both commercial tools and open source software, including [Computer Vision Annotation Tool](#) (CVAT), [Anonymai](#) and [SiamMask](#).

Storage and Access:

Ego4D is not publicly available. Any researcher seeking access to the data must review and formally assent to license terms imposed by each EGO4D partner, which delineate permitted uses, restrictions, and consequences of non-compliance. Access to the dataset is only granted after each university reviews these commitments, through unique credentials which expire after a specified period. Time-limited access controls dataset sharing beyond authorized users bound to the terms of our licenses. Storage of EGO4D data is also regionally compliant with GDPR and other regional requirements. This was achieved by working with the [Common Visual Data Foundation \(CVDF\)](#) where the dataset is hosted.

Use of images of people from dataset:

In addition to redaction and informed consent, we have imposed additional restrictions on the use of images from the dataset. Please reference our data use license to ensure you are in compliance with these legally-binding terms.

Partners:

University of Bristol, UK
Georgia Tech, USA
Carnegie Mellon University, USA
Indiana University, USA
International Institute of Information Technology, Hyderabad, India
King Abdullah University of Science and Technology (KAUST), KSA
University of Minnesota, USA
National University of Singapore, Singapore
University of Tokyo, Japan
University of Catania, Assn. IPLAB c/o Department of Mathematics and Computer Science, Italy
Universidad de los Andes, Colombia

Additional Information: Reviewing boards are acknowledged below,

University of Bristol, [Research and Enterprise Development](#)
Georgia Tech, [Responsible Conduct of Research](#)
Carnegie Mellon University, [Office of Research Integrity and Compliance](#)
Indiana University, [Human Subjects and Institutional Review Board](#)
King Abdullah University of Science and Technology (KAUST), [Institutional Biosafety and Bioethics Committee \(IBEC\)](#)
University of Minnesota, [Institutional Review Board](#)
National University of Singapore, [Research Integrity and Ethics](#)
University of Tokyo, [Office of Human Research Studies](#)
Universidad de los Andes, [Ethics Committee](#)