Interim Report on Proposed Privacy Guidelines for Smartglasses AI

Masahiko Tsukamoto, Masakatsu Morii, Shinichi Kita, Takuya Niikawa, Seiichi Ozawa, Tsutomu Terada, Togo Tsukahara (Kobe University)

July 1, 2025

*This report is based on the presentation made at the JSPS KAKENHI Symposium "The Present State of Smartglasses: Progress Report on Guideline Formulation for Privacy Control and Countermeasures Against Misuse" held at Takigawa Memorial Hall, Kobe University on October 17, 2024.

Currently, the development of smartglasses and AI is remarkable, starting with the introduction of Google Glass and HoloLens, and the demand for consumer glasses like Xreal Light and Air has expanded. In recent years, smartglasses that resemble ordinary spectacles and color pass-through goggles are rapidly growing. Coupled with the improved performance of generative AI, the utilization of AI is expected in various fields such as on-site work, real communication, and daily life support. However, this development has also brought forth significant privacy issues. This paper discusses the privacy challenges of smartglasses AI and proposes concrete countermeasures.

Privacy Challenges of Smartglasses AI

Due to their characteristics, smartglasses AI can pose the following privacy challenges:

- **Real-time data collection and privacy infringement**: Smartglasses have the ability to collect data in real-time to identify individuals and analyze behavior and conversations, requiring restrictions on data collection scope and the formulation of guidelines.
- **Misuse of personal identification and facial recognition technology**: Concerns exist regarding the misuse of facial recognition technology that can easily identify strangers and others. Regulations on the use of facial recognition technology and clear limitations on its purpose are required.
- **Unauthorized collection of voice assistant and ambient conversations**: There is a possibility of constant collection and analysis of ambient sounds, necessitating a mechanism to obtain consent from surrounding individuals.

- **Privacy of gaze data**: Since users' interests, concerns, and emotional states can be inferred, explicit user consent must be obtained, and the scope of use should be strictly managed.
- **Unauthorized information collection and lack of data utilization transparency**: Risks of personal data misuse or unauthorized use exist, requiring transparency and explanation.
- **Data security and leakage risk**: Sensitive personal information may be included, necessitating robust security measures.
- **Social and ethical impact**: The possibility of increased anxiety regarding surveillance in public spaces and the rise of a surveillance society may increase threats to smartglass usage. Therefore, the formation of social consensus and the formulation of ethical guidelines are indispensable.

Concrete Countermeasures for Privacy Protection

The authors are advancing the formulation of concrete guidelines to address these issues and are considering the following seven countermeasures:

1) **Smartglasses Indicators**:

   Proposal: Attach red lines on temples or moderns, or red marks on bridges or frames, visible from both front and side. Indicators showing the presence of cameras or displays are also effective.

   Opinion: Since smartglasses are very powerful tools, it is important to make their presence known to those around them, and there is an opinion that penalties for intentionally painting over or hiding the marks are necessary. It is believed that by integrating it with aesthetically superior designs and applying a unified indicator, it would be easier to handle in examination halls and movie theaters. On the other hand, disadvantages such as design disruption, undesirability for disabled individuals, stalker countermeasures, and forensic use cases are also pointed out.

2) **Operation Indicators**:

   Proposal: During recording or audio capture, a red LED indicator and a chime sound, or a beep sound at regular intervals (e.g., every 3 seconds), should be emitted. When simply powered on, a green light, and when AI functions are in use, a blue light could indicate what the device is doing.

Opinion: There is an opinion that notification functions during recording are necessary and should be made known to those around, similar to smartphone shooting operations. Standardization and penalties for hiding or disabling these indicators are also considered necessary. It is believed that the privacy of the recorded subjects should be prioritized, and it may be sufficient to indicate whether video or audio is being recorded. However, some opinions note the potential for noise disturbance to others and the challenge of publicizing the meaning of the indicators.

3) **Wearing Armbands or Bibs**:

Proposal: Require the wearing of armbands or bibs not only for professional use but also for personal use. Discuss including names or shooting purposes.

Opinion: It is thought that requiring the wearing of bibs for individuals authorized to use AI or record at specific crowded locations by the event organizer could be a good idea. It is also considered effective for public uses such as media reporting. However, concerns are raised that for casual personal use, it could significantly impair the convenience of smartglasses and hinder their widespread adoption, making it too demanding.

4) **Electronic Notification**:

Proposal: Utilize technologies such as specific servers, Wi-Fi beacons, ARP/ICMP to electronically notify surroundings of smartglasses usage status. User names can be anonymized.

Opinion: It is considered useful as a platform for personal information protection law countermeasures. While some believe this is a realistic approach, others argue that the necessity of notification itself needs discussion, and ensuring effective notification and obtaining consent from subjects remains a challenge.

5) **Camera Slide Cover (Lid)**:

Proposal: Install a slide cover on the camera that can be opened and closed manually or automatically.

Opinion: This is considered practical and favorable as it can reduce discomfort, anxiety, and potential disputes among those nearby. The physical lid provides a sense of security, and its necessity is emphasized, especially in public transport settings, drawing parallels with concerns about smartphone cameras. However, some opinions point out the

difficulty of recognizing a physical lid, the risk of damage if dropped, and the inconvenience if smartglasses cannot be used in public without a lid.

6) **Automatic Mosaic**:

Proposal: Automatically apply a mosaic to captured video footage. Allow manual switching and prevent mosaics for registered individuals such as family members. Further advanced AI functions could also be considered, such as not applying mosaics to individuals which indicate "OK to photograph" during shooting.

Opinion: This is considered a promising method that can save the effort of manually deleting personally identifiable information later and avoid privacy troubles. However, technical challenges are pointed out, such as the difficulty of 100% masking, the difficulty of external verification that a mosaic is being applied, the accuracy of facial recognition, and the complexity of real-time implementation.

7) **Automatic Data Encryption**:

Proposal: Automatically encrypt captured video, audio, and biometric data to prevent unintended dissemination.

Opinion: This is considered a desirable mechanism from the perspective of personal information protection, and it is pointed out that companies may already be implementing such measures. However, concerns are raised about significantly impairing convenience, managing decryption, the risk of information leakage to specific organizations, and the possibility that malicious users might not disclose captured images.

Conclusion

The rapid development of AI promotes the utilization of smartglasses, but at the same time, overly powerful smartglasses AI will inevitably cause privacy problems. For healthy development, it is indispensable to address these issues early and formulate guidelines. The seven proposed countermeasures discussed in this paper are concrete steps towards protecting privacy in smartglasses AI, and further discussion is needed in future technological development and social consensus building. In particular, a multifaceted examination is required from both the balance between the privacy of users and the privacy of surrounding individuals being photographed, as well as the technical feasibility and social acceptability.

This research is supported by the JSPS KAKENHI Grant-in-Aid for Scientific Research (A) "Privacy Control Technology for Smart Glasses AI" (22H00550, Principal Investigator: Tsukamoto, 2022-2026).