Ethical Considerations for a New Monitoring System

Glacier National Park Camera System for Monitoring Logan Pass

Created By:
Sophie Brochu, Matthew Catuccio, Ava Chadbourne, Philip Heney, Harish Suresh

Advisors:
Leslie Dodson, Bethel Eddy

Overview

This document contains a list of ethical considerations to be reviewed during the implementation of a monitoring system at Logan Pass. These questions are designed to ensure the safety of any personal identifiable information that may be collected through the cameras at Logan Pass. While not exhaustive, this list contains questions regarding the storage and handling of information, transparency with visitors, the use of artificial intelligence, and potential data leaks.

Most of these questions may be applicable if the Visitor Use Management team at Glacier National Park decides to utilize the 2023 WPI team's proof-of-concept system in its current state. All questions should be reviewed with extra scrutiny when significant changes are made, and when external consultants are utilized.

Questions are divided into **four** main categories:

- Storing and handling Personal identifiable information (PII)
- Transparency in monitoring
- Using artificial intelligence technologies to monitor parking lots
- Potential data leaks

Notes:

- "**Information**" refers to images of the Logan Pass entrance and exit that may contain PII.
- "**Data leaks**" refers to the unauthorized access of private or protected information

PII Storage and Handling

- **Who has access to the information?**
  - Consider all steps that the information follows, from:
    - SD card collection/replacement
    - SD card transportation
    - Data processing
  - It could be useful to keep a list of individuals who may have access to this data in case data gets leaked
  - Will this information be shared with other research groups?
  - Will this information be shared with law enforcement, if requested?
- **Who and how many individuals have access to the information?**
  - Keeping the number of individuals small limits the chance for information to leak
  - Keeping a small group also makes it easier to trace back any information leak
- **Are individuals with access associated with any institutions or organizations outside of the park?**
  - Are they associated with academic institutions or corporations that may want to use or publish this information?
  - Will any of this information be publicly published? (for researchers/students)
  - What are the decision-making processes that might be needed to authorize the use or publication of this information?

PII Storage and Handling

- **How long will this information be stored?**
  - How long are SD cards in the camera?
  - How long are SD cards in transit?
  - Does data processing occur immediately after SD card collection?
- **Will this information be stored on personal devices?**
  - Whose devices might they be stored on?
  - For what reason would they be stored on a personal device?
  - For what duration might this information be stored on a personal device?
- **What safety features are in place to ensure the information does not get leaked?**
  - Is there a safe storage device for the SD card once it is collected?
  - How quickly and thoroughly is the information deleted following use?
  - Are all hand-offs of SD cards person-to-person?
    - If not, how are the SD cards being exchanged?
  - What security features are implemented on the cameras?

Transparency in Monitoring

- **Are visitors aware there are cameras set up to monitor parking lots?**
  - If visitors are not made aware of the presence of cameras, is there a way for them to find out more information?
- **Are employees and volunteers aware there are cameras?**
- **Are visitors and employees made aware of the purpose of the cameras?**
- **Are visitors able to see a sample of what is being collected by the cameras?**
- **Are visitors able to learn how the information is being stored?**

Using AI Technologies to Monitor Parking Lots

- **Does the software access the internet?**
- **What functionality does the software have?**
  - Can it identify objects other than just cars?
  - Can it track specific cars?
  - Can it extract license plate numbers or other identifiable information?
- **Where does the software come from?**
  - Who created it and for what purpose was it made?
  - Was the software created for this specific purpose or a similar purpose?
- **What issue is the software addressing?**
  - Is the software making decisions?
  - Does the issue require human emotion or critical thinking?

Data Leaks

- **Potential areas of data leaks**
  - **Image collection**
    - If cameras are not secure, they can be broken into or stolen. This would result in the loss of the SD card that stores the images
  - **SD card collection**
    - If SD cards are not stored safely, they can be misplaced or lost
    - Any member who collects the SD cards can insert the SD card into their computer and store the images
  - **SD card transition (Time between the SD card collection and Image analysis)**
    - If the SD card is not safely stored, it can be misplaced or taken by an unauthorized individual
  - **Image analysis**
    - If the analysis software is connected to the internet, there is potential for information to be sent through the internet to unauthorized parties