AN EMERGING TECHNOLOGIES, ETHICS, AND RESEARCH DATA CASE STUDY

POLICE BODY CAMERAS

By: Ingrid Skoog
with the Emerging Technologies, Ethics, and Research Data Subcommittee of Harvard Catalyst’s Regulatory Foundations, Ethics, and Law Program

OVERVIEW

The Emerging Technologies, Ethics, and Research Data case studies provide education and guidance on how to identify, assess, and review research data security issues. These studies may be used by IRB administrators and investigators to identify key issues, considerations, and decision criteria when reviewing and designing research studies that involve data collection and sharing components.

Case studies follow a standard format that includes: 1) a fact pattern, 2) contractual, regulatory, ethical, and technical issues, 3) stakeholder considerations to identify, assess, and mitigate risks, and 4) resolution and points for discussion.

By identifying common themes, linking them directly to federal regulations and guidance, and outlining options, the case studies can be used in a variety of ways, which include: 1) as an educational tool for training individuals in human subjects research, 2) as a basis for developing reviewer checklists/worksheets, and 3) as a tool in designing research projects.

We encourage you to reproduce and use these materials freely. In doing so, we require that you acknowledge Harvard Catalyst as the publisher and that you give appropriate credit to the individual authors. For additional information, visit http://catalyst.harvard.edu/about/citingsupport.html.

CASE STUDY

Scenario/Fact pattern:
The study aimed to gather moment-to-moment data of both activities and biopsychological factors to learn more about the specific correlates of stress in police officers wearing body cameras. The study would use administrative data from the police department (e.g., logs of 911 call data, the type of call, dispatches, court appearances, and administrative work) and correlate it with data from a wearable device (including, but not limited to time, heart rate, skin temperature, ambient temperature, galvanic skin response, and accelerometer data). They also proposed an online survey to collect demographic data from the participants.

Officers would be notified of the study via their police department and instructed to reach out to the study created email or phone number if interested. Participants would be required to wear a
Basis Peak, a fitness watch for tracking health and sleep habits, for a two week period. The police department would be asked to supply the research team with administrative records for all officers in the department. The study team proposed that the identities of participants would remain confidential to their fellow officers, management, and in final publication. Only one police department was targeted for this study.

CONSIDERATIONS

Research Considerations:

- Would the team allow review of data by police unit before publishing?
- How can the data be truly de-identified with such a small, targeted population?
- How do they handle the identifiability of those wearing watches? Would it be possible to ask the whole department to wear watches to mask the identity of those participating in the study?
- What permissions would need to be gained from the police union?
- How would the team deal with the privacy concerns of the 911 data?
- Would the introduction of the wearable monitor have any impact at all on job performance abilities in the field? (e.g. distraction from haptic cues, beeping, reminders; interaction with uniform; prohibitive motion, etc.)

IRB Considerations:

- In order to keep identities of participants from management, the study team planned to request all administrative records from the department rather than just those in the study. How does consent work for the non-participating officers whose records are being shared?
- Would utilizing an honest broker/third party to anonymize or code the administrative data prior to receipt by the researchers be a more secure way to use it for this study?
- What if an adverse event happens during the study – will a certificate of confidentiality be enough to protect the police officer from subpoena of data?
- What sort of lead time is necessary for coordination in a study with so many involved parties to get agreement across all participants, vendor, police department, police union, etc.?
- Does the consent form notify participants that third party companies (e.g. Basis Peak) will have access to data about them? Does the consent form contain information consistent with the Basis End User License Agreement language?

IT Considerations:

- How do you keep the participants personal data from the wearable vendor?
- What about technical challenges of participants in properly configuring and using the wearable during the study? Is the research team poised to provide support or would the participant need to reach out to the vendor for assistance? For this study, it was stressed to configure the device so that features such as GPS tracking were turned off – there is a risk that the participants would not configure the device correctly and thus collect unintended sensitive data for the study.
RESOLUTION & DISCUSSIONS

- A certificate of confidentiality was sought to protect participants
- A data use agreement (DUA) was executed between the wearable vendor and Harvard Lab. Basis was to provide bulk download of participants' data based on username at end of the two-week period via encrypted Amazon S3 file transfer.
- Participants were to be given study specific email addresses to use for all aspects of the study. These single purpose research emails were to be used for Basis enrollment.

In the end, the study did not move forward for two main reasons. First, coordination between and authorization from all involved parties was not completed. Second, a recall occurred for the Basis Peak devices due to overheating causing burns and blisters (reference). When using new technology in research studies, it is important to account for these types of potential risk in your protocol.