Improving Privacy Protection for Police Body Camera Systems in Smart Cities

Claire Cochrane
Temple University
Philadelphia, PA, USA
tuf39527@temple.edu

Chiu C. Tan
Temple University
Philadelphia, PA, USA
cctan@temple.edu

ABSTRACT
The main drawbacks of police body worn cameras is the potential threat to our privacy. This article summarizes the main approach towards privacy protections that are used by police departments today, and discusses how advancements in mobile/wireless systems can help improve privacy protections in future Smart City environments.

Keywords
Body Worn Cameras; Privacy; Smart City

1. INTRODUCTION

Recent incidents between the police and general public in Baltimore, Cleveland, and so on have increased interest in equipping police with body worn cameras when on duty. A body camera system consists of two components: a body worn camera unit that is worn on the police officer’s outfit, typically around the chest area, that is capable to recording audio and video from the officer’s point-of-view; and a backend storage facility, such as a off-site cloud facility, that archives the collected video footage to allow future reference.

The idea behind body camera systems is that recorded footage of police interaction with the public, e.g. during a stop-and-frisk, will provide an objective record of transpired events. The recording provides evidence to not only exonerate police officers from false complaints, but also investigate and punish errant police officers. Preliminary experience from pilot body camera deployments also suggests that both the police and public behave better when they know their words and actions are being recorded [5].

The popularity of body cameras have led the concerns about possible privacy violations. Unlike static cameras like CCTVs, body cameras are potentially far more invasive, since the wearer of the camera (the police officer) can capture video from far more locations that are off-limits to CCTVs, such as private homes, restrooms, and so on. Furthermore, due to the nature of police work, both the police officer and civilian may be in stressful situations that make it difficult to make decisions on whether to record footage or not. Finally, pervasive deployment of body cameras give rise to fears of Big Brotherism, where the captured footage will be analyzed to discover infractions long after the fact.

Looking into the future, technological trends like cheaper Big Data storage and more advance data analytics makes it more likely that body cameras like systems will become more ubiquitous in future Smart Cities. It is not a stretch to assume that people whose jobs involved interactions with the public, such as EMTs, security guards, and so on, will be equipped with these cameras. The paper will first summarize the basic privacy protections for existing police body camera systems, followed by a discussion of potential ways a Smart City can help enhance such protections.

2. EXISTING PRIVACY PROTECTIONS

Law enforcement in general are aware of the privacy implications of body worn cameras, and have taken steps to minimize the privacy violations. The distributed nature of law enforcement in the United States means different jurisdictions will have their own guidelines on protecting privacy, and some of these guidelines may differ widely. Based on our investigation of existing police department policies, we can summarize these protections into the following three approaches.

1. Avoid recording sensitive footage in the field.
2. Restrict the access of the recorded video footage.
3. Systematically delete unnecessary video footage.

Due to space limitations, we restrict our discussions in this paper to three localities: Dallas, Tx [1]; Seattle, WA [3]; and Las Vegas, NV [2]. Figure 1 summarizes the main criteria for police to record videos, and Figure 2 summarizes who can access these videos. Figure 3 summarizes how long these videos are kept.

3. HOW SMART CITIES CAN HELP

A key feature of Smart Cities is an environment rich in sensors and actuators. This Internet of Things environment can provide additional “smarts” to improve
privacy protections. One of the main methods is finer-grain indoor localization. The wireless infrastructure in the Smart City can be combined with advance indoor localization techniques [4] to provide more accurate location information than GPS. This fine-grain localization can be used to identify sensitive areas and provide prompts to the officer to start or stop recordings.

Another potential feature is improved context-awareness. Current body cameras require extensive human judgement to record or not. Advancements in wireless networking and cognitive radio technologies in Smart Cities opens up sufficient bandwidth to allow for real-time analytics, e.g. from computer vision, to better inform the officer of potential privacy violations. Offloading technologies proposed for 5G cellular networks can also help promote computational offloading to provide similar contextual information.

Figure 2: Access to recorded videos

4. REFERENCES