Chapter 14
Privacy and Pervasive Surveillance:
A Philosophical Analysis

Alan Rubel
University of Wisconsin – Madison, USA

ABSTRACT

This chapter analyzes some tools of pervasive surveillance in light of the growing philosophical literature regarding the nature and value of privacy. It clarifies the conditions under which a person can be said to have privacy, explains a number of ways in which particular facets of privacy are morally weighty, and explains how such conceptual issues may be used to analyze surveillance scenarios. It argues that in many cases, surveillance may both increase and decrease aspects of privacy, and that the relevant question is whether those privacy losses (and gains) are morally salient. The ways in which privacy diminishment may be morally problematic must be based on the value of privacy, and the chapter explains several conceptions of such values. It concludes with a description of how some surveillance technologies may conflict with the value of privacy.

INTRODUCTION

The potential for continuous, contextual information gathering about individuals, referred to as *pervasive surveillance* or *uberveillance,* adds to the growing list of privacy issues with which contemporary societies must contend, including expanded legal authority for surveillance, growth of relational databases and an industry dedicated to filling them, ease of information sharing in social networks, surveillance initiatives in the service of public health, and sophisticated sensing technologies. Commentary lamenting privacy loss is common, dating back over a century, and many of us are familiar with commentary dismissing concerns about privacy, either on the grounds that we already have no privacy or that we cannot make legitimate claims to it.

DOI: 10.4018/978-1-4666-4582-0.ch014

The purpose of this paper is to analyze privacy claims in the context of pervasive surveillance, drawing on a growing philosophical literature on privacy. Specifically, I address problems related to the concept of privacy itself and problems in determining whether privacy loss is morally important. I will begin by describing a small part of the pervasive surveillance terrain, using examples that will help illustrate several important conceptual and moral problems. I then address the notion of privacy loss itself, offering an account that accommodates the broadest array of conceptual issues. Although it is obvious that pervasive surveillance technologies diminish aspects of privacy, they cannot destroy privacy altogether. In addition to diminishing privacy, pervasive surveillance can actually serve to protect certain aspects of privacy. Indeed, the more important issue is whether pervasive surveillance undermines or protects *morally salient* aspects of privacy. Put another way, whether there are privacy harms, whether privacy claims are impinged, and the extent to which objections to privacy loss are justified depends on the features of that loss. To address that issue, I outline several ways in which privacy loss may be morally weighty and apply the framework developed to some of the ways surveillance technologies may be deployed. I then describe the relationship between the value of privacy and rights to privacy, and conclude by noting the limitations of the analysis offered and directions for further work.

BACKGROUND

Pervasive surveillance, or "uberveillance"—a term developed by Michael and Michael to denote the intersection between automatic location identification, contextual information gathering, and implantable devices—is difficult to pin down precisely (Michael & Michael, 2007). Roughly, the notion is one of widespread and well-integrated information gathering that tracks persons or objects in many areas, and incorporates contextual information. The degree to which contextual information may eventually be incorporated into surveillance systems, the ability for people to create new uses for technologies, and individual willingness to be surveilled is difficult, if not impossible, to predict. This is not an attempt to offer an overarching vision for the direction and future of pervasive surveillance. Rather, in this background section I will draw on the work of others who have analyzed the technological landscape in greater detail and point out some possibilities for pervasive surveillance in different arenas, offering examples of pervasive surveillance technologies that will provide a foundation for the discussions of privacy and claims to privacy in the following sections.

There are any number of technologies that can be developed or deployed as part of pervasive surveillance. A useful starting point is Radio Frequency Identification Devices (RFID). Katina and M.G. Michael have written extensively on RFIDs that can be attached or embedded into objects (for example products in a supply chain for tracking purposes), into animals (for example, into pets or livestock for identification purposes), or into people (for example, into employees for access purposes) (Clarke, 2007; Michael & Michael, 2007). Such devices may be passive, merely providing a unique identifier when scanned by a fixed or mobile reader, or active, recording and/or transmitting information about the condition of the object, animal, or person to which the device is attached or in which it is embedded. The primary implantable devices until now have been passive RFIDs that allow for personal identification and tracking (Kosta & Bowman, 2011; Rotter, Daskala, & Compano, 2008). However, future devices may be able to monitor physiological states of the implantee (Kosta & Bowman, 2011); indeed, one important provider of RFID devices for medical purposes has announced the development of an