

DS 760

Ethical Issues Surrounding Emerging CCTV Analysis in the UK

Rick W. Lentz, M.S., M.S.

15 October, 2017

Issue and Background

When in a public space, you may have seen a public like this indicating that you are being watched:

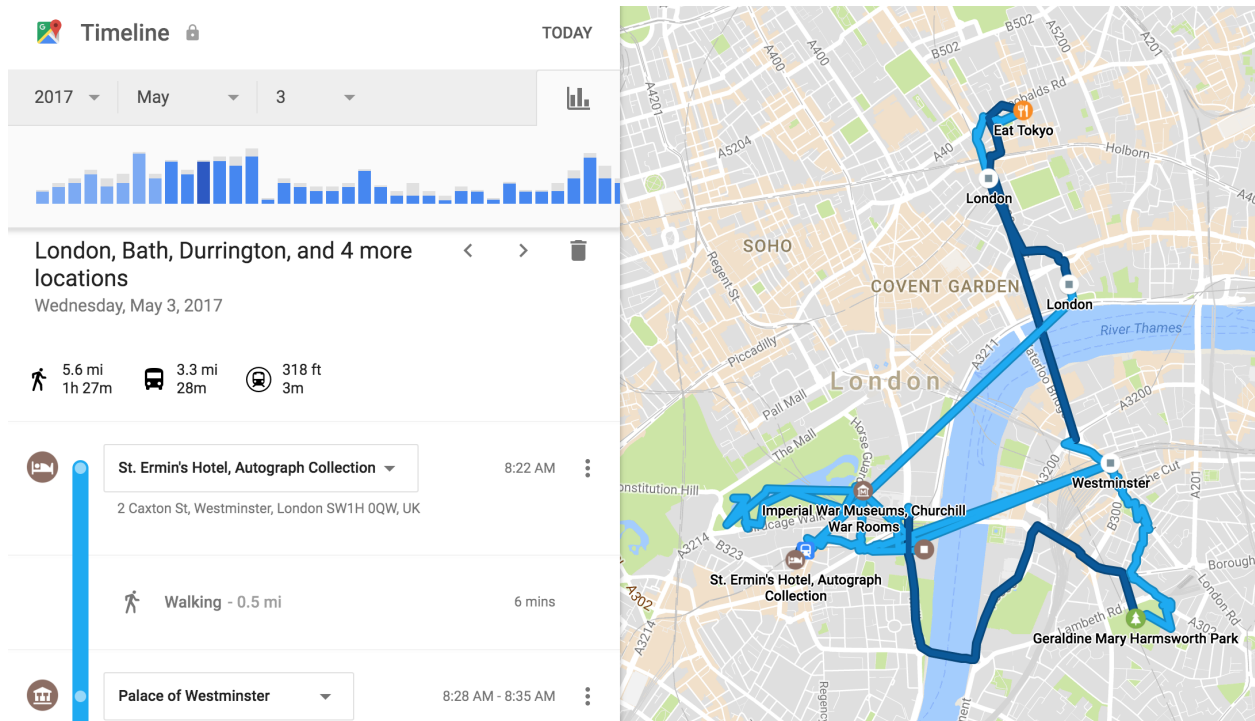


But what about the history of this video or the aggregation of thousands of video feeds that can perform functions other than those listed on this sign?

As introduced in the readings, CCTV coverage in the UK has a sound legal base for policing and intelligence operations. As with many data types, researchers work to improve techniques that unlock new functionality. This paper takes a critical stance on a few methods. These are meant to represent the continual change in capabilities and methods available for CCTV information. This paper concludes with an alternative view and a defense of the alternative view.

The methods of interest in this paper are:

- Tagging of individuals with their real identification information
- Tracking the individual's complete location history over time. Here is a personal example of my 'track' for one of the ten days we spent visiting London earlier this year:



- Automated behavior classification is an individual's higher level activities (Xiang, 2006), social activities, and estimated motivating factors over time (Fig 1 below from Swears, 2014)

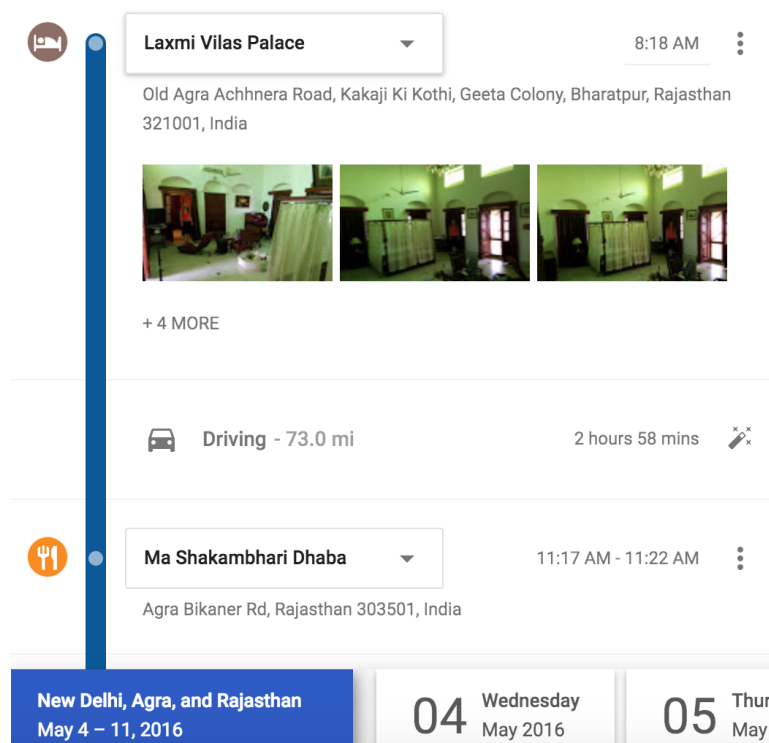


Figure 1: (L) VIRAT Ground surveillance video showing an example of the person-unload-vehicle activity with overlaid annotations and background clutter. (R) Ocean City webcam video with Delivery activity example annotated in yellow.

Critical Stance


Identification or re-identification uses any attributes to link a real identity to an observed object. These can be gait, body shape, clothing, or mobile phone id (since every mobile phone contains a radio fingerprint in its transmission signal which remains unique to that mobile). This use is covered by the Data Protection Act 1998 with one exception. The data has to be held indefinitely though due to the nature of new information having the ability to improve a prior finding (Chen et al. 2017).

Video and devices can also be analyzed to create and generate timelines of an individual's pattern of life. As shown below, this history contains the 'when' and 'where' in an individual's story.



The UK government can gain lawful access to this information under the 1994 Intelligence Services Act.

Regarding Automated Behavior Classification, there appears to be little active dialog regarding its ethical use or use in a security context. From a threat monitoring perspective, this source of information is the highest value. Given the fusion of sources needed, I feel that should be



protected and structured as to be ‘beyond the reach of hackers and insider threats.’ I think Moor would call this “degreasing”.

Alternative Stance

The alternative stance would be Moor’s position regarding the transparency of policy and derivative data use. The three methods would not pass the Justification of Exceptions Principle since the great likelihood of harm would have to be known in advance. These methods work when applied preemptively and independent of any specific individual (Mishara, 2016).

Moor calls for the alterations to be explicit and made public as part of updating the changed rules. This is difficult for me to address, because it appears in the UK, that alterations to these policies are likely restricted under the Official Secrets Act 1889.

Counter to the Alternative Stance

Although Moor has framed the ethical principles regarding protection of an individual’s rights, it is hard to extend these to the protection of the population’s rights, especially within the context of the UK’s National Security Laws. The policy of the UK is to protect sources and methods under the authority of the Official Secrets Act 1889. Thus much public debate will likely be tempered by an uncanny silence, at least from those with actual professional involvement (Dunlap, 2012).