Response to Vallor and Bekey (2017)

Vallor and Bekey (2017) present some of the ethical risks posed by artificial intelligence, or machine learning, systems. Some of the risks outlined include meaningful human control and oversight of these systems, algorithm opacity and hidden machine bias, challenges to economic stability, the design of systems for exploitation, and human overestimation of system capabilities. My concern here is exploring personal privacy as another potential ethical risk, which Vallor and Bekey (2017) do not examine in depth, particularly in regards to privacy spillovers and the ambiguity of property rights over the creation of data within public and private realms.

This risk of potential breaches on personal privacy comes from the notion of privacy as an individual right, as considered in the United States, and also the possibilities of unanticipated repercussions, or spillovers. Tucker (2017) gives the example of genetic data that is uploaded to ancestry services such as 23andme, which not only reflects one individual but also has consequences for family members, since one's genetic data has significant similarity to their relatives–thus creating privacy spillovers. The machine learning algorithms that find patterns to determine ancestry may be accessing unauthorized personal information from the relatives of this individual. Such data may have been captured for one purpose, but may potentially create data about other individuals without them being aware that their data is being recorded.

Furthermore, where traditional legal models of privacy have created a linear distinction between a private realm where an individual can have an expectation of privacy and a public realm in which there can be no such reasonable expectation, such as in the case of *California v. Greenwood* (1988), this notion has become muddied particularly with the use of mobile devices that capture photos and videos. This footage may have been created for a recreational purpose to capture a memory, but creates the possibility of producing data about other individuals whose voices or images may be captured without their awareness and consent. It is not clear how this footage can be definitively disregarded as a context where someone has no right to control creation of data about themselves, i.e. privacy. This kind of data, generated by an individual yet also potentially created about others and used for other purposes, has potential machine learning applications such as the monitoring of public health and other surveillance purposes, further exemplifying that clear lines of privacy is needed within these systems.

References

California v. Greenwood, 486 U.S. 35, 108 S. Ct. 1625, 100 L. Ed. 2d 30 (1988).

Tucker, C. (2018). Privacy, algorithms, and artificial intelligence. In *The economics of artificial intelligence: An agenda* (pp. 423-437). University of Chicago Press.

Vallor, S., & Bekey, G. A. (2017). Artificial intelligence and the ethics of self-learning robots.