Class Activity 1 – Algorithmic Surveillance:

Workplace surveillance 'spiralling out of control'[1]

The intrusive and increasing use of surveillance technology in the workplace is "spiralling out of control", and could lead to widespread discrimination, work intensification and unfair treatment without stronger regulation to protect workers, warns UK trade union body.

The Trades Union Congress (TUC) said the deployment of various digital technologies to monitor workers activities took off after the onset of the pandemic, with employers seeking greater oversight of employees working remotely.

The digital monitoring tools available today – often powered by artificial intelligence (AI) – allow enterprises to see a range of information about their employees' activities, from recording their keystrokes and mouse clicks to tracking their physical location and use of applications or websites.

While the use of employee monitoring tools was already ramping up before Covid-19 – a 2019 Accenture survey of C-suite executives, for example, found that 62% of enterprises were "using new technologies to collect data on their people and their work to gain more actionable insights" – the move to remote working has facilitated a further increase in their use.

In response to a survey conducted on behalf of TUC by Britain Thinks, some 60% of workers said they have been subject to some form of surveillance or monitoring by their employer, with three in 10 agreeing these practices had increased since the start of the pandemic. This marks an increase on the 53% who said they had been subject to workplace surveillance in 2020.

The TUC also found that, outside of workers in the gig economy, the financial services, wholesale and retails, and utilities sectors had the greatest proportion of workers reporting surveillance, at around three in four each.

"Employers are delegating serious decisions to algorithms – such as recruitment, promotions and, sometimes, even sackings," said TUC general secretary Frances O'Grady.

Do you support the development and implementation of the above surveillance systems at workplaces? What are the benefits? What are the risks?

[1] https://www.computerweekly.com/news/252514006/Workplace-surveillance-spiraling-out-of-control-says-TUC

Class Activity 2 – COVID-19 + PATRIOT Act:

Is the COVID-19 pandemic and the crisis around it any different from the 9/11 incident? If they are different, is there an argument that can justify the use of broad warrantless technology-driven surveillance of people (e.g., like what was allowed under the PATRIOT Act) during the COVID-19 crisis that were found to be deeply problematic in the 9/11 context? Why?

Class Activity 3 – Public-Private Partnership around COVID-19:

Should the tech companies and the US government partnered to use geotagged data to identify potential COVID-19 infections and its community spread? Discuss using a Kantian approach, an act utilitarian and a rule utilitarian approach.

Class Activity 4 – MIT's PrivateKit: Safe paths app:

The MIT app called PrivateKit: Safe paths[2] is a tool where an individual, infected by the coronavirus can voluntarily opt-in to share their location data from their phone. The idea is that the app can then track where this infected person has been and who they have crossed paths with. Eventually, the app shares this personal data with other users in a privacy-preserving way, such as those, who are likely to be in the close vicinity of the infected person over a two week period in the past.

The creator of the app, Ramesh Raskar said that: "*People give their stem cells for patients that need a stem cell transplantation. They give their blood. We hope that people think about the crisis, and are willing to give their data."*

Do you think it is an ethically reasonable comparison – that is, is asking someone to share/donate sensitive, personal data same as donating their blood, organ, or stem cells? Why?

[2] http://privatekit.mit.edu/welcome-private-kit