Your face is considered to be PII (Imperva, n.d.). After all, what could possibly be more identifiable to a person than their own face. PII, ethically, and now in many cases legally is to be treated with the highest degree of care. In fact, some places have gone as far as to codify this, e.g., GDPR. If a company starts to scrape images from public sources and then pairs that image with a name then all ideas of privacy have been breached – as it is now easy for anyone with access to the data to get your name and image.

In Hill (2020) the story of ClearView AI is even worse as those images and names are then turned over to the cops. More than likely the police wouldn’t be able to secure that data without a warrant, but because they are using a 3rd party software they are in the clear.

What about real-time facial recognition? Could the police use cameras to search citizens going about their day and then arrest anyone who matches another person with a warrant? Police typically need probably cause to make a stop, is looking similar to a wanted person enough?

Moreover, facial recognition isn’t flawless. Najibi (2020) shows that across 5 different systems females with darker complexion have the lowest accuracy. Darker males are also less accurate than lighter males. These factors could cause more false positives leading to false arrests and detainments.

Hill, K. (2020, January 21). *The secretive company that might end privacy as we know it*. International New York Times, NA. https://link-gale-com.ezproxy.snhu.edu/apps/doc/A611773186/GIC?u=nhc\_main&sid=bookmark-GIC&xid=602284b3

Imperva. *What is personally identifiable information*. (n.d.). https://www.imperva.com/ learn/data-security/personally-identifiable-information-pii

Najibi, A. (2020). *Racial discrimination in face recognition technology*. Science in the News. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology