Microsoft Facial Database Notes

<https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2>

# How it relates to EAD 3 Pillars:

**Universal Human Values:**

There doesn’t appear to have been any attempt to safeguard universal human values. This is due to the fact that the database was publicly available and was able to be accessed by firms such as military researchers and Chinese development companies. We do not know whether these companies had good intentions in mind when using this dataset and there does not appear to have been any attempts to safeguard those whose images appear within the dataset. There is evidence that the Chinese suppliers Sensetime and Megvii are linked to officials in Xinjiang, where the internment camps for Uighur Muslims are based. This is a definite breach of Universal Human Values as the data may have been used to assist in human rights violations that are being perpetrated in that area.

**Political Self-determination and Data Agency:**

The dataset was named ‘Celebs’ as it was supposedly made up of images of public figures. However, a large number of people included in the dataset would not be considered public figures and instead were “merely people who work online and have a digital identity.” This ironically includes Julie Brill, the former FTC commissioner responsible for protecting consumer privacy.

We do not know how many participants granted Microsoft the right to use their image and information, but there were definitely members who were not consulted and had not ceded their right to privacy. This is a violation of data agency due to the fact that this information was used without the subjects’ knowledge and was ‘scraped’ from the internet.

It may also be a violation of Article 9 of EU GDPR: “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.” They were using this information to identify a natural person which is prohibited.

The data was available publicly with no safeguards in place to prevent it being downloaded or used by potential bad actors. This was an infringement of trust not only on those that may have given permission for their information to be used but even greater on those who did not give permission. Microsoft had a duty to keep their information safe but instead they allowed other companies and researchers to use it for unspecified purposes.

**Technical Dependability:**

Nothing really on technical dependability as this issue is not about a specific algorithm or results but more on how data has been taken and shared around the world.

# How it relates to General Principles:

**Human Rights:**

If this data was used by companies to aid in the construction of internment facilities for Uighur Muslims, then it strongly contravenes the International Convention on the Elimination of All Forms of Racial Discrimination, as well as the Universal Declaration of Human Rights. This should have been taken into account by Microsoft when making the dataset public. A recommendation could be that a company declares for what purpose it will be using a dataset of this size and a regulatory body has the decision on whether the company should be allowed to use it.

**Well-being:**

There are arguments that some companies could use this dataset to increase human well-being through the work being done with it that may improve facial recognition accuracy. However, the method that was used to obtain it has certainly decreased human well-being due to the invasions of privacy and lack of Microsoft’s researchers’ integrity. A similar dataset could have been created using subjects that willingly gave their information to be used, however this may have cost more money and, in this case, it appears that Microsoft put economic interests in front of societal interests.  **Data Agency:**

The subjects were not asked for consent and their images were scraped under the terms of the Creative Commons license that allows academic reuse of photos. However, it is very clear that these images were then used for commercial or non-academic purposes by other companies. Although the initial retrieval of the images is supposedly legal under Creative Commons, how does that translate to other companies using information you have gathered for unrelated purposes? Individuals should have data agency over how their information is used and they should have been notified that other companies were trying to use their data, as well as that Microsoft was initially scraping it from the web.

**Accountability:**

Although Microsoft didn’t release an AI system and instead used this dataset to train and research their own, should they be held accountable for how the dataset is shared and for what subsequent projects it may be used for? This may lead to a contentious topic as it could be argued that once a company makes a dataset publicly available it is not their responsibility what another company does with it. However, in this case the original dataset should be made as safe and data secure as possible to prevent future users from taking information they are not supposed to have (such as personal information from subjects within the dataset).

**Awareness of Misuse:**

Microsoft did not make an attempt to notify users that their personal data was being harvested into a dataset. Not only is this a misuse of personal data but also potentially an exploitation of vulnerable users who may not have wanted their information to be widely available. An even greater abuse of trust is the fact that this data was then made available and given to other companies, both domestic and foreign, with no notification to the subjects within who may have objected had they been aware of what was being done with their data.

# Relation to Classical Ethics

**Kantian Ethics:**

“A human has a right to know when they are interacting with AI and may require consent for any AI interaction”, this should also extend to when data is being harvested for use in training an AI system. By denying people the right to choose their data agency, Microsoft has not respected human dignity that humans have a rationally created duty to protect.

**Utilitarian:**

There could be arguments made that making this dataset publicly available leads to greater advancements in AI and machine learning technology that will help people in the long term. However, these companies profit from the development and marketing of these AI systems and the methods that they acquired the data can be seen as negatively infringing on people’s rights in the short term. Utilitarianism wants to avoid short term benefits and, in this case, it could be argued that perhaps the best solution would have been to build the dataset up slowly from people that Microsoft explicitly asked for permission to use their data. In this way, the long-term benefits would have eventually been reached and nobody would have had their data misused or not been aware of how their data was being used.

**Aristotle:**

“Eudaimonia” is the goal of humanity, roughly translated as “flourishing”. There is a strong emphasis on avoiding excess which is common in an economically driven society. Microsoft may have ignored this in favour of obtaining a head-start on training facial recognition AI software by ignoring the data and personal rights of the subjects used and instead were too focused on economic gain.

# Overall

The main issue with this Microsoft case is that the people’s rights were infringed upon and data was taken without their knowledge, used and given to other companies who may have been using it to train systems that perpetuate human rights abuses.   
Microsoft is in the wrong with how the data was obtained and shared publicly without the subjects’ knowledge. A question is whether Microsoft is responsible for what other companies do with the data?