Filipp Krasovsky
University of San Diego
MSADS 501: Foundations of Data Science
Section 2
2-8-2021

Journal Entry 2: The Ethics of Using Artificial Intelligence in Healthcare

I find the consequentialist framework of using private information for the "greater good" (and no other consideration) as unethical on face value. While involuntarily using HIPPA-protected medical data might reduce model training time and increase the predictive quality of an analytics product, it calls into question the obligations a business entity has in using this data to create revenue.

Even in the case that data is used for social good, we run into the risk of it being sold behind closed doors to private companies. Their financial motivations can be directly at odds with the preservation of human dignity. It is conceivable that a beauty product company might target people with skin cancer or other skin conditions to exploit the sense of vulnerability that naturally comes with those medical problems. This practice is unethical because interacting with others on subjects related to one's medical problems can be extremely humiliating – a just society should be able to create an economy that is forced to provide some level of consideration to others without severely restricting economic freedom. Regulation often creates barriers to quickly iterating analytics products, but often at the justifiable cost of reducing the risk of moral harm to others. Meanwhile, deregulation creates more harm at scale – larger corporations that do not face consequences for unethical business practices tend not to be displaced by other market actors and increases in analytical output will not always justify the ethical concerns. With regards to privacy in particular, the well-intentioned nature of AI has been co-opted by state actors (such as the CCP) to identify and punish political dissent through its social credit system. Although this isn't particularly related to the healthcare industry, it's a poignant example of the abuse of AI that occurs in the wrong hands (Ross, 2020). Similarly, in the US, facial recognition technology has led to disproportionate incarceration of African Americans due to faulty modeling, even if the intent may not have necessarily been to disparage any particular ethnic group.

In more research-motivated applications of personal medical data, we can make a moral case for regulation based on the somewhat exploitative nature of private data collection. Insofar as a patient's private information can be used without their informed consent to create a deliverable or product (ie a new drug) which brings in revenue to the entity using the data, it would seem immoral not to compensate the individual who contributed the information. At the bare minimum, however, when compensation on a case-by-case level is infeasible, we ought to at least regulate the practice through mandating informed consent.

With regards to publicly available information, however, the line is somewhat blurred as privacy becomes less of a concern on face value – if we assume a person was aware of the implications of participating in a public space (ie posting their photo on the internet), it's harder to claim undue moral harm on the individual level. Ethical objections to private use of public images and photos are somewhat diminished in this instance; however, government use of facial recognition from public surveillance should face some regulation. In particular, it might be beneficial to demand a very high model performance threshold to be used in a court of law, or as with other common law rulings, to ban the use of statistics from serving as evidence in a criminal trial. At minimum, the source code ought to be

provided to the defense counsel to demonstrate the lack of reliability of an AI module. For instance, if a suspect is indicted based on facial recognition technology, a clever defense attorney could find several people that look very similar to the witness. In the event the technology recognizes some of them as the suspect, or recognizes the suspect under a different name, this provides some leverage to the defendant in pushing back against the charges, although it would still be insufficient in instances where people rely on a public defendant, who often doesn't have the resources to go through this process for all of the hundreds of cases she/he is handling at any given time.

References

Andersen, Ross. September 2020. *The Panopticon is Already Here*. The Atlantic, accessed on 2/8/2021 at theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

Crockford, Kade. June 16, 2020. *How is Face Recognition Surveillance Technology Racist?* ACLU, accessed 2/8/2021 at https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist/