Benjamin McDonnough

Information Privacy

With the rise of new technology and ways of communication, information privacy has started to become a major concern in the tech industry. This can easily be seen in social media, targeted marketing, etc. New technologies that are affected by information privacy are also on the rise, such as brain-computer interfaces (microchips). As Chat-GPT describes in the hypothetical scenario that it created, these microchips can “[collect] and [analyze] their thoughts and emotions in real time” (Chat-GPT). Creating a moral way to decide which part of this information is private has been a contested discussion point.

The thoughts of the users are by far the most private part that is being collected in the hypothetical scenario. Thoughts can only be known by the person that is thinking them unless told to someone else. Therefore, in order to be more ethical and not use peoples’ thoughts to use for “targeted advertising, market research, and even influencing their behavior”, companies should not have access to peoples’ thoughts without the person making that choice for themselves. (Chat-GPT). The taking of information should be governed by the ethical idea of subjective relativity. People should have the option to “[decide] right or wrong for himself or herself” (Quinn, 118). While the technology might be beneficial to some, it can be very harmful to others.

Since it is not feasible for one governing body to decide what is best for every individual person, it should be up to the individual people to decide what is best for them. It might be very beneficial to someone to have their information shared in order to be helped or treated. However, it can be detrimental to others for a multitude of reasons. Moreover, it is against the Constitution to “force” self-incrimination. This means that companies couldn’t use the information collected to be able to incriminate someone since it would be self-incrimination. Also, companies having the ability to “control” thoughts and emotions has a massive impact on how people live from day to day. People can be heavily influenced to buy a certain product, support a certain brand, or even vote for a specific political candidate.

This idea of subjective relativism also trickles into things like social media. While it may not be able to access somebody’s thoughts, it can access patterns in likes, searches, and viewing history. This information is also used for things like targeted marketing. It is also used for spreading information that is either misleading or wrong in order to sway people who are seeing it to do a certain thing. These videos/posts are stemming from the social media platform companies taking information from users and using it to fuel what they are seeing. An example of this is TikTok. In the Privacy Policy of TikTok, it is described that TikTok automatically collets information such as “IP address, user agent, mobile carrier, time zone settings, model of your device, the device system, network type, device ID’s, your screen resolution and operating system, ap and file names and types, keystroke patterns or rhythms, battery state, audio settings and connected audio devices” (TikTok Privacy Policy). While there are some things in this list that are sensible and required for normal operation of the app, there is no reason that the app should be tracking things such as keystrokes and file names. This is private information that the user should be able to provide access to at their discretion.

To conclude, information privacy should not be governed by one small body, but each individual person for themselves. This will allow companies to still get important information, while also not intruding on personal information without clear permission. This is an issue that is important to fix now as the devices being created are becoming more and more personal and able to collect personal information.