

James Dixon

CSCI-234-40 -- Ethics in Computing

It is true that within the last ten years, we have become increasingly dependent and reliant on internet technologies and this growth shows no signs of slowing down. This transformation is incredibly powerful, but also terrifying on many fronts. On one hand we are lucky enough to live in a time and place where devices are cheap and the internet is relatively fast and mostly uncensored. On the other hand, we have seen an equally huge rise in tracking, advertising and manipulation (both human and artificial). Despite this, many of us continue to use these services and continue to feed companies our data, either knowingly or unknowingly. Although the subject here is Facebook, on any given week, they can easily be substituted for any of the other massive tech corporations like Google, Microsoft or Amazon just to name the big ones. They all share similar anti-competitive business practices and view data collected from their users as an asset. It has been proven time and time again that these companies are not afraid to trample on people's privacy for an opportunity to make profit and when that happens it turns into an ethics problem.

Granting an app permissions on your smart device can be a tricky thing to do these days as it seems they are always doing something nefarious with it in the background. The Facebook app is certainly no exception to this as seen in the Computer Weekly article. Giving the app permission to use one photo means it has access to every picture you have ever taken. The same goes for Location as well, granted you have it turned on. The amount of data generated and stored by the average smartphone user is staggering and can help a company infer a lot about someone's life, financial status, friends, relationships, etc. This type of advertising based on vast amounts of collected data has become the industry norm and continues to fund the companies that control the internet. The tradeoff here is one where people trade convenience for their

privacy. Personal information can either be used for things like user studies, performance monitoring, or other such improvements, but it can also be sold en masse or auctioned off. The real issue is that data collection is opt-out rather than opt-in for many operating systems and applications which is simply unacceptable.

There are many examples of the unethical manipulation of content shown on digital platforms that have been reported like Facebook's use of the news feed to affect users' moods. As the paper on ethics states "When designing a new computer system, the professional must consider not only the specifications of the client but also how the system might affect the quality of life of users and others" (M. C. Loui and K. W. Miller). These experiments are dangerous and irresponsible as there is no way to know that state of mind of the person in the experiment for example they may be depressed or suicidal. On a larger scale, Google has been known to manipulate search results for elections based on their own political agenda. A relevant Bible verse concerning this is "Whoever can be trusted with very little can also be trusted with much, and whoever is dishonest with very little will also be dishonest with much." (Luke. 16:10).

In any online social platform there is always the issue of people who want to game the system for profit or influence. The longer the platform exists, the more people can figure out the inner workings of the algorithms that control it. In Facebook this manifests as the "fake like" problem. This is an ongoing issue and will only get worse as AI gets more and more advanced.