To Post or Not to Post

Bradley Harper

Cookeville, TN

[brharper42@tntech.edu](mailto:brharper42@tntech.edu)

Privacy is a topic discussed far and wide. How much privacy should a person have? How much privacy is too much privacy? Should the government regulate and administer the privacy of its people? What information should be kept private? Where do we draw the line between the information we share and the information we keep under lock and key? The social contract, which is an abstract, obligatory document, may hold the answer to many of these questions. Social Contract Theory as a workable ethical theory relates to two major factors according to [1]; these factors are: “ (1) the establishment of such a set of moral rules to

govern relations among citizens and (2) a government capable of enforcing these rules.” By connecting a few dots, it is possible to adopt privacy into the social contract, but how far can this boundary be extended? Some would say that most, if not all, information should be public domain. Others would argue that even just family photos share an excess supply of information to someone with deviant acts in mind. This idea should be further developed upon by seeing just how much information is shared publicly, how that information is/could be used, and how ethical the use of such information really is.

Facebook is one of the largest social media platforms to this day. It is a place where you can share your most cherished details such as family photos, things you enjoy, places you’ve been, places you’re going, people you’re with, Farmville gifts, and so much more. What a convenience! Why bother remembering where you’ve been when Facebook can do that for you. According to Kashmir Hill in [2], a private company, Clearview AI, “scraped the open web of public photos — from Facebook, from Venmo, from Twitter, from education sites, employment sites — and had a massive database of billions of photos”. Using these photos, the private company offered the police a system of face recognition like none other. The moral conundrum in this case is represented best by deciding if this kind of technology is trusted to be used by only law enforcement. Hill continues by discussing how someone could use this facial recognition if it were available to the general populous. Providing some examples of how the data could be used against an individual, Hill contributes details of how “anyone can know who you are any time they’re able to take a photo of your face”. Direct access of your information such as friends, family, and location would make deviance a mere walk in the park. Going back to the social contract, this would be considered unethical due to having no opt-out option available. The facial recognition software rips the privacy from under an unsuspecting and downright unwilling citizen. The societal code may alter slightly were this to happen, but people probably would still upload their content nonetheless. After all, who’s worried about a stranger on the subway knowing who I am?

[2] also talks about how cold cases have been solved using this application by Clearview AI, sometimes only needing a portion of someone’s face. It could see a person in background views of other photos and even “solved a case within 20 seconds,” reports [2]. After seeing so many law enforcement firms using this application, Hill asked to have her photo run through to find zero results despite having several photos of herself online. She also had an unidentified officer run her photo through as well, and he was contacted shortly after by Clearview AI to be questioned about it. This information would lead to the assumption that Clearview could not only privatize results, but also see who was looking for such answers. The social contract does not cater to a biased search, and in turn, shows how unethical this practice is. The unidentified officer in [2] resumes by saying that his account had been deactivated and that the officers were “not supposed to be talking to the media”. Hill asks one final question to the officer about if the trade-offs of the app are worth the infiltration of privacy. His response, in brief, says that yes, so long as it’s being used for the right reasons.

Whether something is ethical or not seems fairly opinionated. After all, the theory of relativity doesn’t refer to just one scenario. If the application catches criminals, it must be good. On the other hand, if the application were to magically come up with no results for a criminal, then either the criminal really had no photos, or worse: the parent company is hiding information. [2] has already demonstrated the ability to hide results using Clearview. This can be seen as very unethical in what in can be used for. The social contract holds a clear connection between the set of rules set by society and a government that can enforce it. Clearview AI, being a private company that avoids both societal decisions as well as government rulings, is an obvious crossing of the social contract.

Each person can decide their own rules of privacy of course. Whether you decide to be a social media butterfly, or a hermit that does not want to be displayed online at all is entirely up to the individual. What you provide is entirely up to you. Therefore you can consider not posting as a method of opting-out. In many cases, it is possible to set filters to what information can be seen and by who. Although, a person should not feel that posting vacation pictures of their family is a threat to the safety of that person’s home and belongings. In cases such as [1], maybe a “bug” in the system will protect you. Who is to decide, aside from Clearview A.I. of course?

[1] M. Quinn *Ethics for the information age,* 7th ed. Hoboken, NJ, USA: Pearson Education Limited, 2015, pp. 80-83.

[2] A. Brown and K. Hall speakers, “The End of Privacy as we Know It?”*, The Daily,* Feb. 10, 2020. New York City, (NY): The New York Times. [Podcast]. Available: <https://podcasts.google.com/feed/aHR0cHM6Ly9yc3MuYXJ0MTkuY29tL3RoZS1kYWlseQ/episode/Z2lkOi8vYXJ0MTktZXBpc29kZS1sb2NhdG9yL1YwL3Y1aVM4TElzNi1HbGI2ZHJEX1FidkltSGNxTTNMT0E0OHctdnRwdDhhOWc>. [Accessed Oct. 22, 2020].