Atticus Emilsson

PHIL 355E

Module 1

1.4 Case Analysis on Privacy

In the case presented by Vaidhyanathan in *The Googlization of Everything (And Why We Should Worry)*, many instances of individuals voicing their concerns regarding Google Street View (sometimes referred to as GSV) can be observed. Some of these concerns revolve around Google Street View compromising their safety by providing valuable layout and architectural details that may be of benefit to burglars. Most of the concerns are more so related to Google Street View invading their privacy in a manner that does not allow for much choice. Google has demonstrated a behavior that closely resembles the belief that it is "easier to ask for forgiveness than to ask for permission" by handling privacy concerns in an asymmetric manner. We see varied implementations of Google's privacy-enhancing technologies depending on certain legislation, but a complete lack of respect for privacy in a societal context. In this case analysis, I will argue that Utilitarianism shows us that Google should have used its vast resources to explore the privacy implications inherent in the design of Google Street View and methods to offset these risks.

In Luciano Floridi's book *The 4th Revolution,* he attempts to explain why privacy is "one of the most obvious and pressing issues in our society." To determine a satisfactory and reproducible explanation for this issue, one must define a method for measuring privacy or an

action's effect on privacy. To achieve this, Floridi introduces two concepts that are often used in accordance with one another, which can be described in a manner that is similar to electrical current and electrical resistance. He coins the term "informational friction" which he defines as the forces that "oppose the flow of information within a region of the infosphere." He also uses the term "informational flow" often. This informational friction can be compared to electrical resistance, and the term informational flow can be compared to electrical current. By using this definition of informational friction, we can measure how previous technology has impacted privacy and combine this information to predict future privacy implications that a technology might introduce.

Floridi also recognizes the inverse of the privacy implications introduced by these technologies. In the case of someone less technologically inclined, it is much more difficult to protect themselves from these implications. On the other hand, somebody who is more technologically inclined will not only be able to increase the informational friction from their end but also use these technologies as privacy-enhancing tools. This increased reliance on social media and other technologies that enable such elevated levels of interconnectivity means that someone might be able to manipulate their true image. Privacy-concerned individuals who wield some advanced degree of technical knowledge can create sock puppets (a fake digital identity, typically used in online investigations) and employ other methods for masking/disguising their online presence. One can also employ a method that is described as "poisoning the well" where incorrect information is used to mask accurate information. Just because these methods for protecting one's privacy are possible, does not mean they are plausible.

One main argument made against Google in the case of Google Street View is that during its conception, not enough effort was made to increase the information friction between sensitive components of people's private lives and the public. They did blur faces and license plates per the requirements of local legislation (like in Canada) but did not employ this by default until later. They also boasted about having an opt-out feature where individuals could "request that an image be removed;" however, the process was time-consuming and difficult. This means the image remained on the internet for an unknown period and took some technical expertise to quickly and successfully opt out of the service. Viewing this situation through a Utilitarian lens, one can aptly determine that Google's action of implementing a difficult and flawed opt-out procedure in Google Street View did not minimize suffering. There are some simple implementations of these aspects that exist, such as making the opt-out process more user-friendly. This would enable most people to increase informational friction in a way that directly benefits them while having virtually no impact on anyone else. This would protect the sanctity of their privacy, thwart potential bad actors, and be a comparably cost-effective solution to the privacy issues presented by Google Street View.

This point is similarly touched on by James Grimmelmann in his writing relating to *Privacy as Product Safety*. Viewing privacy through a lens of product safety does not fully encapsulate the issues presented; however, it does provide a stepping stone for identifying flawed designs that may have unintended implications. Examples of these issues are provided in the writings. Google Buzz was a highly integrated social platform pushed by Google. These platforms inherently decrease informational friction, so certain precautions must be taken to protect end-users. Google Buzz's implementation was incredibly flawed in multiple ways and

introduced users to unforeseen implications, some of which could have been potentially life-threatening.

One feature of Google Buzz that is an outright violation of privacy is the contact listing feature. Google Buzz would list a user's most contacted individuals on their profile. In the case of one user, Buzz revealed a woman's current partner to her abusive ex. This could have led to the harm of her current partner or revealed an avenue for discovering information regarding her current whereabouts. This issue is exacerbated by the highly integrated nature of Google's ecosystem, which even enabled Google to create Buzz profiles for people who never outright registered. These privacy implications could pose a massive threat to the safety of citizens and informants, the integrity of journalists, and the confidentiality of political communications. Revisiting Grimmelmann's model of viewing Privacy through a lens of product safety, it is incredibly clear that publishing an individual's frequent contacts should require a clear understanding of the implications and explicit permission from the individual in question. He emphasizes that Facebook will be used in "complicated ways, sometimes leading to privacy trouble," and these tendencies will absolutely carry over to other platforms. Facebook faced a similar issue with its Beacon advertising program, where it leveraged this highly interconnected nature of the internet to scrape and aggregate information from users of other platforms without their explicit consent. In most cases, these users were completely unaware this was happening.

Google Street View shares similar aspects in this regard, especially considering its default non-censored philosophy. The service takes a snapshot in time, documenting individual activities as they remain oblivious. Like Google Buzz publishing a user's contacts for everyone

to see, Google Street View is documenting what other people are doing and uploading it for anyone to see. Although blurring technology may protect somebody from being identified by facial recognition technologies or by their license plate, there are still other ways to identify an individual. This can have severe implications for the individual being documented. They can be recognized by an abusive partner or their vehicle with a specific design be identified at their home by a stalker, all from the comfort of their own home. These issues coupled with the flawed opt-out design and their tendency to publish such information by default rather than obtaining explicit consent will maximize suffering. Viewing these implementations from a Utilitarian perspective, Google Street View poses a massive threat to one's own safety and autonomy. The looming threat of being documented and published directly encroaches on the happiness of the individual. Considering the inherent nature of GSV eroding the informational friction that exists between individuals and the world, assessing the nature of the product's safety in a more interpersonal context would have proven to be less detrimental to individual privacy.

Google has a massive quantity of resources but has consistently proven that they are incapable of predicting the privacy implications inherent to its designs. Both Floridi and Grimmelmann introduce methods of empirically observing and measuring the potential privacy implications that a product might present. These issues are not inherent to Google. Facebook has also exhibited an inability to protect user privacy through confusing implementations and inherently flawed designs. This issue will not go away as we continue to strive towards such a highly integrated world for the sake of convenience. Unfortunately, there is only a certain degree of privacy that can be achieved with these technologies that exist to increase the flow of information; however, that does not mean that one cannot minimize the privacy implications that

these technologies introduce. Rigorous scrutiny of the design complexity and inherent implications can help mitigate the dangers that might be posed to the end-users. This should be of utmost importance, considering that these individuals generate revenue for these organizations.