## PREFACE: DEFINING PRIVACY

The first step in evaluating “entitlement to privacy” is determining what privacy in an “increasingly connected world” entails. Most consider privacy as freedom from observation, but privacy embodies a much more nuanced position when spaced across private, public, physical, and digital spheres.

Within Judith Jarvis Thomson’s “The Right to Privacy,” her primary example is a man with a pornographic image, and how his wishes determine his entitlement to privacy. If he wishes not to share it, but someone looks nonetheless, that is a breach of privacy. If he wishes to share it, and someone looks, that is a waiver of privacy. But as she zooms out, and sees that this is also a question of ownership, she concludes that the right to privacy is actually a cluster of rights: for Muslim women, searching for their uncovered knee is not only a violation of the right to privacy, but also the right to their bodily autonomy; for people with sensitive information, torturing them till they speak is not only a violation of the right to privacy, but also the right to not be harmed; for the man with the pornographic image, looking or touching his image is not only a violation of the right to privacy, but also the right to ownership and the autonomy that accompanies that.

Carissa Véliz’s “In the Privacy of Our Streets” probes more about the space that privacy occupies and is permitted in. One of the key distinctions she draws is the difference between what’s conventionally known as private space and privacy. Though we often associate the two together, it can lead to the myth that privacy is eliminated from public spaces. However, in cases such as mothers finding privacy in public spaces like malls away from their private spaces with children, public spheres can allow privacy, meaning that there is still entitlement to it there. She does, however, acknowledge that the difference from privacy in private and public spaces, is access, and known risk to that access in public spaces, but how that cannot be completely reliable because access is able to be bought out and traded for targeting those who cannot afford private spaces.

Extracting from these sources, we can create a framework for defining privacy: the relationship of conscious intention to divulgence between all parties, contingent upon the situation, space, and time.

## THESIS

Though readings such as those from Jarvis Thomson and Véliz dissected privacy in terms of the definition's latter in situation and space, time is much less discussed. The reason for this may be because until the emergence of this "increasingly connected world," there hasn't been as great of a need for the question of endurance in privacy, since information was rarely preserved in such pristine condition as it is in the digital network, i.e. though privacy across time is still a question for archaeologists who may find human remains or read historical diaries and accounts, it is not of the same intimate condition and volume as instances such as consistent surveillance of a person's entire life. Because of that, my argument will **disagree in that there is an <u>immediate</u> entitlement to privacy,** but **agree that there is no entitlement to privacy in the increasingly connected world when put into the perspective of <u>time</u> and <u>scale</u>.**

## IMMEDIATE ENTITLEMENT

To more clearly outline the terms of immediacy, it means that there are no **foreseeable** breaches of privacy in the near future if the data collected is used for the purpose intended, and solely for the purpose intended, and if the data collected is done so in the way that is established and known to a willingly conscious and consented participant.

The direction that the MAPPING Brown project is currently tracked towards seems to be very conscious and precautionary with participants' immediate entitlement to privacy. They acknowledge the risks of location-based apps and how that can entangle their participants in location-based dilemmas, such as cross-sections in crime scenes and participant locations; they seem to aim to mitigate this through de-identifying, which will also help prioritize cumulative behavior from individual behavior.

Looking at this, people are, in a way, objectified and anonymized into data points, which, from a privacy viewpoint, protects unwarranted intentions in information leakage. This precautionary approach demonstrates **data is still able to be collected and measured on topics like connection and migration patterns without revealing individual habits or location behaviors**, enabling participants to feel secure that their right to privacy is still intact, or as waived as they wanted it to be. MAPPING also allows participants to opt in, and claims to be transparent on exactly what they're tracking, which further protects not only participant privacy, but also knowledge of entitlement to privacy.

## ENTITLEMENT AFTER TIME AND SCALE

---

Though participants are entitled to immediate privacy as outlined in regards to the established study, there's no way to fully predict the manipulations of the data in the future, and that's where the question of time and scale are brought up. Outlining the question that time and scale poses is really outlining what the lifespan of agreed privacy is.

Participants agree to relinquish their location data in the MAPPING project, whether anonymized or not, on the grounds of understanding that this data is going to be used for research on epidemics and pathogen spreading in relation to social migration patterns. The existence of this data in our current networks means that there is a higher chance that it is able to be pulled from the archives for future uses on epidemics. The ethical questions raised are: What did the participants actually sign off on? The experiment is intended to track social migration patterns *in order* to limit others' future behaviors - would they want their data to be used that way? Is their entitlement contingent on their personal anticipation of future manipulations of their privacy? Is the sign-off on this data forever, but only for epidemiological research? While it's easy to "cop-out" and simply create a warning for participants when they are signing off, the truth is that, in an "increasingly connected world", it is highly unpredictable, particularly beyond lifespans - hypothetically, how would participants feel, knowing that their data resulted in a completely brutal massacre 300 years later because this specific data set triggered results that indicated social migration was bad, and the government decided that that was the only solution? We can see here that entitlement to privacy is also somewhat tied to a feeling of responsibility: sometimes we choose to keep things private because we don't want public responsibility, so how can we justify breaching that privacy? What happens when the patterns revealed aren't ideal - can we withdraw our privacy waiver? (Is that really a direct causation of our relinquishment of data and privacy, or would it have happened anyways with passive surveillance, i.e. card-swiping indicating location at a certain time?)

Part of this justification in overriding entitlement to privacy is the concept of a social contract, which is particularly critical in the increasingly connected world. The social contract essentially is an implicit agreement in a society to cooperate for benefits, and this can include sacrificing personal principles for the greater good. In order to reap the benefits of the increasingly connected world, people are generally expected to contribute to it as well; in this case, for the value of greater **scale** health information, perhaps that privacy sacrifice is necessary, if not inevitable. Or when applied to the idea of how **time** inevitably decomposes our entitlement to privacy, we can see it as our legacy contribution to epidemiologic research that hinges on the connected world.

Even in compiling research done prior to collecting this specific dataset, the MAPPING Project participates in using data who's privacy entitlement has been eroded. When it draws from data sets from previous research, Brown has no way of knowing that the participants of the previous research consented to their data being used years down the line. Moreover, if the data set is used in the specified paper, and another paper cites that paper, there isn't a way to constrain the privacy there either. This means that in an increasingly connected world, once that privacy is waived, there is no undoing that in the face of time and scale because access to that data isn't confined.

**SUMMARY OF IDEAS**

---

The central idea is that an increasingly connected world depends on social contributions derived at least partially from data collection, and on a world-scale and on world-time, we aren't entitled, or even capable, to inhibit that connectivity advancement using the withholding of our individual information and privacy. The Brown MAPPING project may do its best to serve our individual right to privacy, but it is ultimately a data collection for epidemiologic research that would be used on the general public. Our rights to privacy are valid on an immediate scale in self-protection, but erosion by time and overriding by scale of that entitlement is an inevitable effect of connection.