SAMPLE A Paper

Morally Evaluating End-To-End Encryption

In 2018, at least eighteen individuals were lynched in India after rumors about them spread across WhatsApp.[1] As the platform uses end-to-end encryption, it does not retain access to the contents of communications. On one hand, this system can be abused to catalyze mass atrocities. On the other hand, encryption allows WhatsApp's 1.5 billion users to communicate freely with each other without fear of undue surveillance.[2] This incident highlights a moral question: is it ethical for a company to enable end-to-end encryption, and if so, what framework should we use to make such a decision?

In this paper, I will attempt to establish and justify a framework for morally evaluating a company's decision to enable end-to-end encryption. In order to build this framework, I shall draw upon the social contract tradition of philosophy and politics: society exists as per an implicit social contract that works to maximize the common good for its members.[3] We can thus judge a company's decision to enable end-to-end encryption based on how well the outcome allows said company to uphold this social contract. Specifically, I propose three heuristics on which to base this, forming the framework we can use for evaluation: (i) the company should uphold the contract between itself and its users by protecting their freedoms, (ii) the company should uphold

[1] "Whatsapp Sets New Rules Amid Mob Killings". 2019. BBC News. Accessed February 9 2019. https://www.bbc.com/news/world-asia-india-44897714.
[2] "How Whatsapp Makes Money". 2019. Investopedia. Accessed March 1 2019. https://www.investopedia.com/articles/personal-finance/040915/how-whatsapp-makes-money.asp.
[3] Celeste Friend, "Social Contract Theory". In The Internet Encyclopedia of Philosophy. Accessed February 8th, 2019. https://www.iep.utm.edu/soc-cont/#H3.

the contract between itself and the government by handing over useful information for individuals who have violated the social contract, thus foregoing their right to privacy, and (iii) the company should be able to hold users liable for violating their social contract with the company in cases of abuse. Along the way, I will examine, through a moral lens, the various societal interests at play in such decisions, including the value of privacy, and the role of national security and law enforcement. I will then consider two potential arguments against this framework to expose its limitations. Finally, I will apply our framework to WhatsApp's decision to enable end-to-end encryption. Given the philosophical focus of this paper, I will assume that technical factors are handled optimally, including the company's implementation of encryption and the security of its data centers.

Let us first establish some background on the social contract theory and how it ties into our task. As Socrates argued, by simply being members of a society, its constituents implicitly agree to a social contract, which is supposed to maximize the collective 'good' for its signatories; in the typical case, each signatory gives up certain rights in exchange for certain liberties and assurances.[4] Law enforcement, the justice system, and militaries, exist then as part of the state's role as a defender of the public interest in this social contract. However, it is important to establish here that the public interest is not simply equivalent to the protection of life. As an admittedly extreme example, if a country were to force each individual to live within the boundaries of their own fortified barricade to optimally protect them, would that be a valid fulfillment of the state's role? Certainly not, because these individuals would have to forego many liberties, and boil life down to a matter of simply staying alive. I believe that upholding the social

[4] Ibid.

contract encompasses the protection of 'human security' in the fullest sense, by not only guaranteeing the protection of life but also allowing the pursuit of other liberties and freedoms.[5]

As entities operating within a specific society or a country, companies are also then a signatory to this social contract. Note that while there are arguments against the coherence and usefulness of social contracts, I am basing my argument on the premise that, regardless of its desirability, through the accepted formation of a society, by Socrates' aforementioned argument, there already exists an implicit social contract between entities willingly operating as part of this society, including companies, users, and governments.[6] With this in mind, one way to evaluate a company's decision to encrypt is based on how well the outcome would allow the company to perform within the context of such a contract - that is to say, how well the company's position on encryption would allow it to protect public interest.

Note that our framework's reliance on the social contract means that it assumes that the state would truly be acting in the best interest of its people, upholding its end of the social contract. Thus, this framework is only suited for societies where democratic institutions are developed enough for the legal system to adjudicate fairly in line with a respect for human rights. However, this still leaves out the fact that socio-political climates evolve, and alongside them, evolve the needs of the people. For example, if a state begins to devolve towards authoritarianism, it would be essential for the company to still honor its social contract with its

[5] "Human Vs. National Security | Global-E". 2019. 21Global.Ucsb.Edu. Accessed February 9 2019. https://www.21global.ucsb.edu/global-e/april-2018/human-vs-national-security.

[6] Celeste Friend, "Social Contract Theory". In The Internet Encyclopedia of Philosophy. Accessed February 8th, 2019. https://www.iep.utm.edu/soc-cont/#H3.

users, as the user would not have done anything to violate their end of the agreement or to justify stripping them of the liberties that this social contract would allow them.

Having established this background, we can now move on the three tenets of our framework. The key idea uniting these is that, to uphold its social contract with the state and its people, the company's decision on the subject of encryption must not infringe upon human security, which we had previously established as the goal of the implicit social contract. However, in exploring this goal, we will have to revisit the moral dilemma at the heart of this paper - that between privacy and security. The tenuous relationship between these forces will be further explored within the tenets of the framework itself.

As the first tenet of our framework, I hold that the company's decision must uphold the contract between itself and its users, by safeguarding its users' freedoms. This is where we consider the value of privacy. If we do not enable encryption, it could allow law enforcement to protect lives by preempting attacks. Perhaps the infamous 'nothing to hide' argument, examined and rebutted by Solove, could be channeled to suggest that individuals who are doing nothing wrong should not have anything to fear from surveillance.[7] However, this position does not hold up to scrutiny: through Bentham's idea of the panopticon, we know that the mere existence of infrastructure that can allow surveillance can cause individuals to restrict their behavior.[8] This would thus represent a breach of freedom for every single user of the service. To contain this situation as much as possible, the company should work to safeguard its users' privacy by

[7] Solove, Daniel J. Nothing to hide: The false tradeoff between privacy and security. Yale University Press, 2011.
[8] Foucault, Michel. Discipline and punish: The birth of the prison. Chapter 3. https://foucault.info/documents/foucault.disciplineAndPunish.panOpticism/

retaining and allowing access to as little information on user activity as possible. Although I leave the question of determining the exact balance for this up to the company's discretion, this will be discussed further at the end of the second tenet, where we further explore the value of law enforcement and national security.

As the second tenet, I propose that, assuming the government is upholding its end of the social contract, the company should honor the contract between itself and the government as well. It can achieve this by handing over useful information on individuals who have violated the social contract. Note that due process is established as part of the social contract itself; if the relevant bodies suspect someone to be guilty of violating the social contract, that individual can lose their prior expectation of privacy, as this had been granted to them through this contract, and they had chosen to forego this by committing a crime. Furthermore, by handing over information regarding violators, the company could help keep the rest of its user-base safe. However, to do this, the company must be able to access useful records regarding user activity. Thus, the company would have to determine how much information to store such that it can fulfill both, the first, and the second tenet, by being able to provide as much privacy to users as possible, while still retaining enough information that it would be useful to law enforcement for prosecuting violators. The question of what this balance might be would depend on a number of factors including the kind of data the company is dealing with, the potential for abuse, and the type of user-base. I thus leave the precise balance between privacy and security up to the company's discretion of what the common good for their users might be.

As a third tenet, the company should also be able to hold users liable for violating their social contract with the company. This point is rather simple: users should be able to point out

or report cases to the company where the platform is being abused. This brings us back to the unfortunate situation we discussed in the very beginning of this essay: fake news leading to lynchings in India.[9] By simply claiming that communications are encrypted, a platform should not be able to eschew its role in helping individuals. However, when the company upholds its social contract with its users, there is a reasonable expectation of reciprocity; indeed, this expectation is what the principle of the social contract rests upon. Thus, when a user defies this expectation and abuses the company's platform to propagate violence or infringe upon the rights of others, as in the aforementioned example, the company should be able to hold them liable.

These three points make up the framework that we can use to evaluate a company's decision to enable end-to-end encryption. We can now discuss some arguments against our ideas to expose some of their limitations.

Firstly, consider the idea shared by Kosinski et al., Solove and Electronic Frontier Foundation that even if certain records seem innocuous, they can be aggregated to reveal personal information regarding individuals.[10, 11, 12] To echo one of the Electronic Frontier Foundation's examples for this, consider that a user's metadata over a 2-hour time period shows a received phone call from a hospital, an call to an AIDS Information Clinic, and then a call to their spouse.[12] Even though we only have metadata records to refer to, we can still reasonably guess the contents of their conversation, infringing upon their privacy without directly recording their

---

[9] "Whatsapp Sets New Rules Amid Mob Killings". 2019. BBC News. Accessed February 9 2019. https://www.bbc.com/news/world-asia-india-44897714.

[10] Kosinski, Michal, David Stillwell, and Thore Graepel. "Private traits and attributes are predictable from digital records of human behavior." *Proceedings of the National Academy of Sciences* 110.15 (2013): 5802-5805.

[11] Solove, Daniel J. Nothing to hide.

[12] Opsahl, Kurt. 2013. "Why Metadata Matters". Electronic Frontier Foundation. Accessed February 9 2019. https://www.eff.org/deeplinks/2013/06/why-metadata-matters.

calls. While this is a formidable argument, in our case, as we have previously explored, we only support allowing access to data for individuals who are suspected of a crime following due process. The social contract argument of them giving up the civil liberty of privacy by choosing to commit a crime would hold in that case.

I would like to establish the next argument against this framework by example. Consider that the Pakistani army were to pressure the legislature into issuing a warrant against a journalist who was criticizing them. They then present this warrant to your company to receive information regarding the journalist in order to coerce them. In this case, even though due process would appear to have been followed, the journalist's right to privacy would be infringed upon, despite her having upheld her end of the social contract. As mentioned before, I believe this framework works best for democratically-developed countries with strong legislative branches, where the social contract between the state and its civilians is upheld. However, the concession is that the framework falls short of protecting the rights of civil society in non-democratic regimes.

Having finished explaining and defending our framework, we can apply this to WhatsApp in the United States as an example. The state has a democratically-developed government, upholding the social contract with its people as expected. Our framework can thus be used to assess this case. With regard to the first tenet we discussed, it seems that WhatsApp does uphold its social contract with its users by encrypting the contents of their communications, allowing them the freedom to communicate knowing that their messages cannot be perused. Moving on the second tenet, it seems that WhatsApp securely retains metadata for communications, and there exists some evidence that they have handed over such metadata to the FBI in certain

cases.[13] Given that a large part of the NSA's surveillance program was built on metadata, this seems to be a useful tool for national security concerns.[14] Finally, consider the third tenet: being able to hold users liable for breaking their social contract with the company. WhatsApp also seems to pass this criterion as they allow users to report other users for abuse, and have been encouraging the use of this as a tool against the spread of fake news.[15] Thus, as it stands, WhatsApp's decision to enable end-to-end encryption seems to satisfy our criteria by upholding its social contract towards the aim of preserving human security.

Embracing the inherent contradiction between privacy and security, we have tried to strike a balance between the two by invoking the implicit social contract existing between individuals, companies, and governments, coupled with the value of human security. We then considered the example of WhatsApp as one possible configuration of encryption that would satisfy our framework. One limitation is that this framework comes with the inherent limitation of only applying to states where the government upholds the social contract. While we attempt to patch this problem through a fluid 'balance' which changes with the country's context, this could be an avenue for further research.

---

[13] "Forget About Backdoors, This Is The Data Whatsapp Actually Hands To Cops". 2019. Forbes.com. Accessed February 9 2019. https://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/#706864c81030.

[14] "Leaked NSA Document Says Metadata Collection Is One Of Agency's 'Most Useful Tools'". 2019. Business Insider. Accessed February 9 2019. https://www.businessinsider.com/nsa-document-metadata-2016-12.

[15] "Whatsapp FAQ - Tips To Help Prevent The Spread Of Rumors And Fake News". 2019. Whatsapp.Com. Accessed March 1 2019. https://faq.whatsapp.com/en/android/26000216/?category=5245250.