The modern-day equivalent of the USA founders' search and seizure is an almost Orwellian fear of the government. Much like that from the eerily visionary *1984*, governments like that of the UK have the ability to constantly surveil citizens, and organizations like the NSA have monitored the calls and messages of US citizens. The worry of George Orwell is reflected in the citizens of the world, as technology capable of almost constant observation has led to these individuals' uncertainty and distrust in the government; however, a government security official would argue that this surveillance is directly correlated with higher public safety. Should a government be able to monitor its constituents or even have access to personal messages, videos, or street that are generally in a private context?

As is in the case of WhatsApp's continuation of end-to-end encryption, tech companies must value the costs of security, the company's subsequent role as a tacit contractor for the government, and the value of its consumers' privacy. An entity like WhatsApp must choose who its constituents are, and then secondly decide what impact this lack of encryption will have on the security and privacy of global citizens, be it positive or negative. I will begin by determining why this is the natural structure in which an ethical framework must be constructed and transition into a discussion how to evaluate the moral role of a technology company. To sum out the central thesis, I will illustrate how the company can potentially evaluate the eventual impact of a universal store of consumer data and private information.

As with any argument, we must elucidate the definitions and assumptions that are central to this thesis. End-to-end encryption is specified above and mentioned throughout the paper, but this thesis will be generalizable to a method allowing an entity to obfuscate the personal audio, video, or text messages of its consumers. This form of technology hides the information channels between any two parties from any entity, including the organization that offers the service and

authorities of any government, which would allow for the hidden, anonymous communication between parties across the world. An important definition that will be used later is that of "privacy" which defined by Alan Westin is "the claim of individuals to determine for themselves when, how, and to what extent information about them is shared with or communicated to others."[1] This definition insinuates that individuals who have private data have full control over all of their data, and there is full disclosure between an individual any party using the data. After understanding the definitions, we must look at why this framework is built in this specific way.

We must understand why any tech company should concretize who its constituents are and determine the net utility of any impact stemming from the expulsion of technology like end-to-end encryption. In any ethical argument, what a company has the responsibility to do is related to the individual entities for which it is responsible.[2] A company can decide to pursue a utilitarian approach to serve the entire world or a primarily business-driven approach to please its direct consumers and preserve their direct ethical interests. Secondly, an organization like WhatsApp must critically reason about any cost-benefit analysis that involves the removal of end-to-end encryption. Will such a diversion lead to widespread benefits, a potential for international harm, or a balance of both? The first two factors relate to determine who the company would be responsible for, while the last two refer to a cost-benefit analysis.

The first major factor to be considered is whether a company should value its consumers' views on privacy over global security implications. The American public has "long been divided in their views about the trade-off between security needs and personal privacy," but there was a general trend after 9/11 (in specifically the US population) approving of government data

[1] Westin
[2] Porter

collection.[3] However, there is a general sense, especially after the Snowden case, that the American public disapproves of the surveillance possible through the end of WhatsApp's encryption, as 53% disapprove while 40% approve the NSA surveillance of telephone calls and internet data.[4] Also as Balkin asserts, Facebook and by proxy WhatsApp are "information fiduciaries" that "must be loyal to their clients' interests."[5] Assuming the a technology company has a pure role to its consumers, the company should not discontinue its use of end-to-end encryption based on these statistics.

However, a dissenter to this consideration may assert that through a utilitarian lens, one should ignore the public opinion by handing over a secret key to governments that exposes a myriad of data points. With this argument, saving these lives and preventing data acquisition by malicious parties far outweighs the theoretical distrust caused by the removal of end-to-end encryption and the passing of this "secret key."[6] The key rebuttal against this centers around distrust. In a theoretically ideal government, this surveillance will be used perfectly to eliminate terrorist threats without any bias, but a slippery slope of increased surveillance can result in dystopia. A precedent of surveillance may allow abuse of power in future governments, even in a country that has been touted as "free." This debate is furthered in the next factor that discusses the myriad of constituents affected by the release of end-to-end encryption.

The second criterion to consider when releasing the use of end-to-end encryption is how the constituency will develop for a multinational company like WhatsApp. With over a billion users across the globe, WhatsApp has a theoretical duty towards the citizens of every country in the world. So how will WhatsApp decide which countries have access to suddenly unencrypted

[3] Manian
[4] Ibid
[5] Heller
[6] Nakashima

data? A company becomes a tyrant if it provides certain pieces of citizen data to some governments but not others, but it runs the risk of handing off relevant, private information to malicious governments to exploit. In addition, different countries have differing views on what privacy means. Bygrave postulates that there are "variations in perceptions of the degree to which interests that compete with privacy…warrant protection at the expense of privacy interests" and these differences complicate the arena in which these privacy games play.[7] According to Bygrave, there is essentially a different theory of privacy, so there must be a different claim to privacy for individuals and governments across the world, complicating the idea of data revelation. Deciding the countries that are granted access to a secret key proves complicated with the changing nature with how people interact with privacy, and there is a clear potential for negative impact when any government can access international data.

One natural opposition to this beam of the ethical framework is the fact that WhatsApp is an American company and should thus only serve the American government. After all, despite a checkered history of immoral dealings with opposing governments, the American government has been one of the most stable, with a general desire to spread freedom across the globe. If WhatsApp is an American company, why can't they help the USA do their "duty" to help the entire world? A rebuttal for this can be seen through an international lens. WhatsApp has a huge contingency of consumers that exist in nations around the world. If data of these users is handed over to a government that does not have a social contract with, there is a clear and obvious infringement on user trust and a bias in users. WhatsApp will unevenly provide certain governments with the tools to monitor and, thus, affect the lives of individuals outside of the sovereignty while ignoring any other government. A clear conflict of interest exists if WhatsApp

[7] Bygrave

truly considers itself an international company; as an American company, WhatsApp could potentially choose to assist and uncover data to the US government, but will run the risk of losing user trust and disproportionately affecting non-US consumers. Even if the US can only see the messages of US citizens, there is an imbalance in the privacy protections of WhatsApp users.

After determining constituents, WhatsApp must determine the ethical implications and impact of releasing the end-to-end encryption. For the third factor under consideration, how is the privacy of the individual user affected by a technology company sharing private messages with third parties. This privacy, as stated by Nissenbaum, has become more "complex online because of shifting recipients, types of information, and constraints under which information flows;" the rapidly growing speed at which computation, querying, and information generation is possible has lead to a complicated web of information pockets that store the personal details of our global citizens.[8] Nissenbaum asserts that as more and more people are connected, there are an increasing number of data points stored altering one's privacy. In the presence of end-to-end encryption, the information flow is siphoned between two parties and is untapped by any other party. In this theoretical setting, the third parties that are granted access to the data of WhatsApp users infringe on any claim to privacy. Westin's definition of privacy as self-determinant falls when a technology company is allowed jurisdiction over personal data to provide to others.[9] To reiterate, when this encryption is removed, WhatsApp is given the responsibility to distribute and provide information channels that contain consumer data; this is a clear violation of Westin's claim to privacy. The consumer no longer determines much about their data at all.

A critic to the previous factor pertaining to privacy will point to the fourth factor to consider in WhatsApp's evaluation of end-to-end encryption. As stated by Solove in "Nothing to

[8] Nissenbaum
[9] Westin

Hide," a common argument is that "the privacy interest is minimal, and the security interest in preventing terrorism" is paramount; Solove continues to state that most feel that the information collected by the government is generally uncompromising.[10] Solove's primary argument centers around the feeling that some are not affect by data collection and processing. The potential benefit from WhatsApp's cooperation with third parties could prevent potential worldwide tragedies and would be a tool used by governments to theoretically better the lives of their citizens. The most recent example of this is through the NSA's PRISM program, in which data is released to the US government in order to help prevent terror across the globe. PRISM "compelled" companies like Google and Skype to hand over transcripts and video call data that was used internally in order to prevent various terrorist attacks .[11] The US government has stated that "over 50…potential terrorist attacks" have been stopped with the institution of heightened US surveillance after 9/11 and the US government values every resource afforded to them.[12] With the help of a technology company like WhatsApp, the US government would have the ability to uncover the secret plannings of nefarious entities across the world.

Another perspective to this final factor may state that the US government has been unsuccessful in the past with certain advances and covert operations and using the privacy data of either US or non-US citizens may negatively affect innocent individuals in an extremely personal way. As stated by Rob Reich, there could be a "loss of freedom, intimacy, [and/or] control over self and future." In addition, Solove continues in his "Nothing to Hide" argument that the "aggregation" of data and "exclusion" of data can construct the private dealings of individuals from innocuous data and affect them directly.[13] The most relevant response to this is

[10] Solove
[11] Greenwald
[12] Savage
[13] Solove

simple; in a theoretical, philosophical sense, we must trust our governments. In a classical sense, governments exist in order to benefit the citizens that exist in it. We agree to exist within some framework of laws and limitations and are then afforded some protection in the form of safety. Even though the US government has a checkered past in foreign relations and covert operations, it has the conceptual intent to improve the lives of individuals existing inside of its sovereignty. When considering this fourth criterion, opposition against a tech company's data provision can be shown that this is a mere extension of a stronger social contract.

Speaking holistically, a technology company like WhatsApp has a multi-branched decision tree in which it must consider various factors that challenge and uphold the continuation of any message encryption. Along with Whatsapp, other tech companies like Skype and Google have major ethical implications with any encryption software that makes it impossible to expose personal messages. These companies must first decide who they are responsible for and then what the overall impact of any action is. The executives of a technology company deciding to end its use of end-to-end encryption must weigh who they are optimizing for and how this optimization will then occur. The ethical implications of end-to-end encryption are endless, and any tech company must wrangle with how its consumers' data is used and stored in an ever increasingly connected world.

Works Cited

Porter, M. E. (2006). Strategy and Society: The Link Between Competitive Advantage and Corporate Social Responsibility. *Harvard Business Review,*78-81.

Bygrave, L. A. (2010). Privacy and Data Protection in an International Perspective. *Stockholm Institute for Scandinavian Law*.

Greenwald, G., Ackerman, S., Poitras, L., MacAskill, E., & Rushe, D. (2013, July 12). Microsoft handed the NSA access to encrypted messages.

Heller, N. (2018, April 13). We May Own Our Data, but Facebook Has a Duty to Protect It.

Maniam, S., & Shiva Maniam. (2016, February 19). Americans feel the tensions between privacy and security concerns.

Nakashima, E. (2016, April 12). FBI paid professional hackers one-time fee to crack San Bernardino iPhone.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online.

Savage, C. (2013, June 18). N.S.A. Chief Says Surveillance Has Stopped Dozens of Plots.

Solove, D. J. (2014). *Nothing to Hide The False Tradeoff between Privacy and Security*. New Haven: Yale University Press.

Westin, A. F. (1968). Privacy And Freedom. *Washington and Lee Law Review,25*(1).