Social Contract Between Users and Social Media Platforms: An analysis of Personal Data Privacy on TikTok

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Hana Kontrec

Spring 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Sean M. Ferguson, Department of Engineering and Society

STS Research Paper

What seems like every few years, there is an emergence of a new viral social media platform. From Facebook, Twitter, Instagram, and Snapchat to Musically, Vine, and now, finally, TikTok. TikTok is the newest in-trend social media platform created by a very successful internet technology company headquartered in Beijing: ByteDance. The platform promotes creativity and self-expression by allowing users to create short form video content. Even though the platform technically launched in 2016, it has seen immense growth in the last couple years, even reaching a billion downloads by February 2019 (Beutell, 2020). This success does not come without any controversy, however, as the company has faced public backlash as well as governmental regulation as a result of their mishandling of user data and poor data privacy practices.

Unfortunately, TikTok is not the outlier in the industry. Data privacy online has been a constant issue throughout the years and has become increasingly harder to manage with the emergence of 'big data.' The phrase "data is more valuable than gold" has been floating around in recent years which underscores the importance of data in the tech industry. It might be free to open up and use a social media account, but the true price you pay is actually your data. Social media companies such as TikTok as well as big tech giants like Google rely on data. That is how they make their money.

Social media platforms have an unprecedented number of users, with this number growing higher every day. Many people choose to participate in this technology without fully understanding the terms and conditions that they are agreeing to. Most users are unaware of how their data privacy can be put at risk on these platforms but choose to participate anyway. In this

paper, I am going to explore the issue of data privacy on social media through the lens of a social contract relationship between social media platforms and their users. I will further explore current legislation of data privacy and propose possible ways forward when it comes to regulating personal data privacy on social media.

The Social Contract Framework

I used the lens of a social contract between a provider and shareholders in order to examine data privacy and the relationship between users and social media platforms. First, according to this framework, when users post their information online, they have a set of privacy expectations that they expect will be respected by the provider. These privacy expectations or norms center around three concepts: type of information, who has access to it, and how it is used in the given community (Martin, 2016). Social media platforms often obfuscate how user data is being used and provide few, if any, opportunities for users to control their data privacy. Facebook, for instance, offers few controls for users to manage how their data is being used. Their focus is mainly on giving users the ability to manage who in their network sees their content and not the ability to manage their preferences on how Facebook itself might utilize their data (Nandon et al., 2018).

When it comes to these privacy expectations laid out by users, there are a couple things to keep in mind. First, everybody is different, therefore, everyone's definition of privacy varies and different users have different thresholds when it comes to what data they are willing to give up in exchange for being able to participate in social media. What is really important to take away is that this perception of privacy can be altered. It has been shown that incentives can influence the way people perceive privacy. Factors like health benefits, convenience, and necessity make a

user more likely to use a technology while lack of trust, online discrimination, and online harassment are disincentives. One might be more amenable to using a smart watch that tracks their steps, heart rate, and other physical data if it helps them lose weight while they might be less interested in getting a smart security system because of a fear of someone hacking into their home system, whether this fear is rational or not does not matter (Xue, 2020). Second, it has been shown that data type is also a significant factor when it comes to what information users are comfortable with sharing. On social media people often post photos for their friends and even the public to see. Some people do not mind that their data is being collected on social media in order to personalize the advertisements and actually prefer it to impersonalized ads. However, when it comes to their browser data and chatting history, users tend to be more fearful and tentative of handing over this type of data (Xue, 2020). Overall, it is important to understand the different facets of privacy that differ user to user and how that can affect their views and their behaviors on social media.

Moreover, privacy as a social contract focuses on informed consent and the contractor's right of exit. Informed consent means that the user is clearly and sufficiently informed about the terms of the contract and can therein make an informed choice to enter and/or exit the contract. The way that social media platforms communicate their practices to users is using Terms of Service and End User License Agreements. This proves as an inefficient method for communication as the majority of users ignore them. Even those who are willing and interested in reading these documents come away dissatisfied and with a feeling like there was no actual choice to decline or negotiate their consent (Nandon et al., 2018). Furthermore, the right of exit is hard to accomplish when it comes to social media. At this point in time, if you disagree with the terms and conditions put forth by a social media platform, your only course of action is to not

use that platform. With social media becoming so ingrained in our culture, users are not often willing to do this which trap them in a conundrum between sacrificing their data or completely opting out.

Finally, social media companies have a responsibility to shift their focus from merely trying to clearly communicate their business tactics to consumers to also managing the expectations of their shareholders and gain consent of the individuals to the responsibilities of the firm as a contractor to maintain a mutually beneficial and sustainable solution. It is not enough for companies to inform their consumers of their practices. Companies can have bad practices and clearly communicate them to consumers but this would violate their responsibility to protect their users' privacy to an expected degree as part of this social contract (Martin, 2016).

Another underlying stakeholder that is important to mention in the scope of a social contract framework is the government. The government, through the use of legal institutions, is an important adjudicator of the terms in the social contract and its aim is to fix any inequalities that arise between the two parties. There is a clear asymmetry between users and social media platforms when it comes to user data. The user is often left in the dark when it comes to knowing and understanding how their data is being used and collected on these platforms. In order to fix this knowledge gap in the social contract, the government has a role in regulating such discrepancies in power.

Case Study of Data Privacy on TikTok

Even in its short-lived lifespan, TikTok has seen its fair share of controversies. As a result, there have been a number of attempts at regulation in different countries. Countries like the United States decided to instate a temporary ban on the platform while other countries opted

for legal regulation. For the scope of this paper, I am going to specifically focus on the European Union's (EU) General Data Protection Regulation (GDPR). Furthermore, I am going to explore the accusations that TikTok is not doing enough to protect the rights of children on their platform. The keystone case for this accusation being the Federal Trade Commission's (FTC) case under the Children's Online Privacy and Protection Act (COPPA) in the US. Overall, the FTC case will be used to outline the issue of children on TikTok and whether or not they are able to participate in the social contract. The GDPR will be explored as a possible guideline in the future to structure proper and effective legislation for the regulation of data privacy on social media as outright bans on social media platforms have been criticized for being ineffective and problematic.

In February 2019, the FTC sued TikTok for a record 5.7 million dollars under COPPA for the allegation that TikTok had questionable practices and loopholes when it came to their registration process for children and their child privacy protection policies. Unfortunately, regardless of the lawsuit and negative press, the platform showed "no sign of slowing down its usage amongst children and teenagers." To put this into context, like mentioned before, TikTok reached one billion downloads in 2019 and 40% of those users are under the age of 24. Even when not taking into account the possibility that many users lie about their age, this accounts for roughly 400,000,000 users! TikTok groups their users into 3 categories: children (under 13 years old), teenagers (between 13-18), and adults (18+) (Beutell, 2020).

According to TikTok, children must obtain parental/guardian consent to use the platform and will only have a limited access to the platform. Teenagers must also obtain parental/guardian consent but will have access to full features and content of TikTok as the adult category. There are many issues with this. Once the app is downloaded you are prompted to make an account.

Once an account is made you can use the application with no limitations. You are not prompted to conform your age until you "update" your profile (Beutell, 2020). Moreover, parental/guardian consent is never actually confirmed by the platform. In the worst-case scenario, this means that a child under the age of 13 can freely use the application without any limitations without any parental/guardian consent. This is especially troubling when noting the fact that once a user makes an account on the platform, their data is immediately being collected and stored by the company meaning that the company is collecting data on minors and using it for financial purposes (i.e., personalized content, advertising, …).

This brings us back to the discussion of the social contract where social media platforms have the responsibility to clearly and effectively state their business practices. The "Terms" stated in the TikTok Privacy policy are legally binding "between you and us" and you may not access or use the app if "you are not over 13 or otherwise able to agree to these Terms" (TikTok, 2021). While the above set of rules is stated clearly in their privacy policy, is stating them this way enough to gain proper consent from minors? Moreover, a 2017 Deloitte survey revealed that 97% of users between the ages of 18-34 do not read any Terms of Service they agree to (Beutell, 2020). If almost all young adults fail to read the Terms of Service documents, how can we expect these policy documents to be sufficient enough to get proper consent from minors? TikTok should be doing more to protect younger user's data privacy and access to the platform. Confirming a user's age online is a difficult thing to implement. It would either include platforms like TikTok checking user ID's or other personal documents or having a national database of people and their ages. Both are unrealistic and would result in numerous other privacy concerns. However, social media platforms should at least shoot for implementing the bare minimum. In the case of TikTok, this would include prompting a user to confirm their age during the process

of making an account. This is not a perfect solution, but it is one step closer to maintaining a mutually beneficial and sustainable solution to dealing with younger users on such a platform.

As mentioned before, ByteDance, the parent company of TikTok, is a company based in Beijing, China. In 2019, TikTok got into hot water over a possible national security risk that could affect US user data. TikTok was accused of sending "vast quantities of private and personally-identifiable user data" to servers in China. This is troubling due to the fact that the PRC has national security laws in place that could compel any company to participate in 'intelligence work'. This means that the Chinese government can request any TikTok user data contained on Chinese servers and TikTok would be lawfully required to hand over this data and restricted from publicly speaking about it (Ryan et al., 2020). The company claimed that no US user data was being stored in China, but regardless, in December 2019, the US Army, under the guidance of Pentagon, banned the download and use of TikTok on government-issue devices and encouraged employees to cease their use of the application (Anderson, 2020).

As a result of this controversy, the Trump Administration banned TikTok in the U.S. by issuing an Executive Order cited to powers granted in the International Emergency Economic Powers Act of 1977 (IEEPA). This was a controversial move not only in its effect on the tech industry but critics also referred to it as an "overreach of executive power – the kind that the IEEPA intended to prevent." While the ins-and-outs of the IEEPA are outside the scope of this paper, it is important to note that the IEEPA was created in order to limit executive power but, in recent decades, has been increasingly used by presidents to further their own foreign policy objectives (Faison, 2021). The importance of data privacy is not an issue that can be solved by the IEEPA because the IEEPA framework does not allow Congress a big enough role in regulation to make any real change. Simply put, other than reviving and deciding to allow or veto

the current ban under the IEEPA every 6 months, Congress essentially has no real input in the regulations put in place under IEEPA. Data privacy is a complex issue that needs to be solved by equally complex legislation that provides comprehensive and long-term solutions. This would require Congress to have a big role in future regulation of data privacy on social media.

In order to solve this problem, the government could look to other countries for inspiration and guidance on how to begin shaping regulation about data privacy so that it is more comprehensive and effective. Unfortunately, data privacy on social media has largely been neglected by legislation and even legislation and laws that have been passed to deal with the problem "have no teeth." One step closer to improving current privacy protection laws is the recent passing of the EU's GDPR. One of main principals of the regulation is "that a person is the owner of [their] data and [they] have the right to decide who can use it and how" and "regardless of where and how the data is shared, it can be amended, deleted, or [one] could determine who and how it would be accessed" (Desai, 2019). The regulation places financial penalties on companies that are found to break the principles outlined in the regulation and TikTok has already been sued by countries like France and the UK for millions of dollars. The GDPR gives users the power over their data. In the scope of a social contract, the GDPR helps close the asymmetrical knowledge gap between users and social media platforms when it comes to the knowledge of and access of user's data. It makes social media platforms more responsible for managing user data as well as properly informing the user what data they are collecting, for what purpose, and giving the user an option to delete their own data or opt-out of specific data being collected from them. The regulations aren't perfect and there are criticisms on both sides of the aisle. Some argue that the GDPR is doing too much while other argue it isn't enough. Regardless, it is the first of its kind that truly gives the user some power over their data on social

media and it is definitely a good springboard for future legislation in the U.S. and all over the world.

Regulating social media platforms will be a tough and long road for the U.S. government given how fast the technology is growing and evolving. However, their obvious lack of progress when it comes to regulation of data privacy on social media, and online overall, is unacceptable and it should become a priority. Moreover, some of the moves made by the government in the past are questionable and they indicate a lack of thought for possible consequences that might exacerbate the problem even further. For instance, the aforementioned ban on TikTok has been shown to be an ineffective solution to attacking the problem of data privacy on social media. A ban on a social media platform could "have a profound impact on the future of an open Internet, technology innovation, and TikTok users' freedom of speech" (Wang, 2020). A ban on TikTok could have negative effects on the open Internet because it is a form of censorship by the government. If we allow the government this ability to censor social media platforms, which platforms are next? Will this censorship extend to other technologies? Something needs to change and looking towards passed legislations like the GDPR that have proven to be somewhat successful will put the government one step closer to tackling this complex issue.

Looking to the Future

TikTok, as a social media platform, has far to go in fixing their relationship with their users in the scope of a social contract framework. A large portion of its users is very young and it comes into question whether these users are even old enough to consent to this contract. Moreover, this isn't just an issue involving younger users. Even older users fail to understand the implicit contract they sign when they agree to participate on this social media platform. Many still do not understand how their data is being collected and utilized when they are online as

TikTok has unclear and obfuscated privacy policies and clearly does not have the best interest of their users in mind when it comes to protecting their data. Even in the best-case scenario, where users are completely aware of the consequences of using social media, they still lack the ability to negotiate. If they do not agree to the terms and conditions of TikTok their only option is to not participate, therein their right of exit is denied. Even further, the government has not done a great job in regulating these social media platforms like TikTok. Overall, the social contract framework points out many different flaws with the technology of social media as a whole. However troubling, knowing these flaws is half the battle. Lessening the knowledge gap will give all the different stakeholders in this relationship a fairer shot at fixing these issues. If users and the government are more aware of how social media platforms are overstepping their power, then they will be in a better place to address it.

Data Privacy on social media is a hard topic to tackle. Analyzing TikTok has shown just how big of a problem regulating data collection and privacy on social media has become. Many current laws often fail to include any regulation regarding data privacy and even those that don't haven't proven to be effective. TikTok has done the bare minimum to fix some of its mistakes in light of lawsuits and bad press which just underscores the importance of the government to step in and do more. The GDPR has proven the most effective in putting regulations in place regarding data privacy and it will be an important document to reference in the future when we are aiming to design more comprehensive and long-term solutions. Furthermore, it will take the full efforts of all branches of the government to tackle this issue. Data privacy is not a problem that will go away in the future, if anything it will get worse, therefore, building blocks need to be put into place now before things get out of hand.

References

Anderson, K. E. (2020). Getting acquainted with social networks and apps: it is time to talk about TikTok. *Library Hi Tech News*, *37*(4), 7–12. https://doi.org/10.1108/LHTN-01-2020-0001

Beutell, J. M. (2020). *Children's rights and social media: An analysis of TikTok's Terms of Service through the lens of a young user*. https://www.ideals.illinois.edu/handle/2142/106069

ByteDance. (2021). *ByteDance.com Privacy Policy*. https://sf16-sg.tiktokcdn.com/obj/eden-sg/upsnuhpevbn/bytedance_official/PrivacyPolicy_ByteDance.com.pdf

Desai, B. C. (2019). Privacy in the age of information (and algorithms). *Proceedings of the 23rd International Database Applications & Engineering Symposium*, 1–12. https://doi.org/10.1145/3331076.3331089

Faison, A. (2021). TikTok Might Stop: Why the IEEPA Cannot Regulate Personal Data Privacy and the Need for a Comprehensive Solution. *Duke Journal of Constitutional Law & Public Policy Sidebar*, *16*, 115–145. https://scholarship.law.duke.edu/djclpp_sidebar/197

Martin, K. (2016). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, *137*(3), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Nadon, G., Feilberg, M., Johansen, M., & Shklovski, I. (2018). In the User We Trust: Unrealistic Expectations of Facebook's Privacy Mechanisms. *Proceedings of the 9th International Conference on Social Media and Society*, 138–149. https://doi.org/10.1145/3217804.3217906

Ryan, Fritz, A., & Impiombato, D. (n.d.). *(PDF) From banning to regulating TikTok: Addressing concerns of national security, privacy, and online harms*. ResearchGate. Retrieved April 8, 2021,

from https://www.researchgate.net/publication/344584442_From_banning_to_regulating_TikTok_Addressing_concerns_of_national_security_privacy_and_online_harms

Wang, J. (2020). *(PDF) From banning to regulating TikTok: Addressing concerns of national security, privacy, and online harms*. ResearchGate. https://www.researchgate.net/publication/344584442_From_banning_to_regulating_TikTok_Addressing_concerns_of_national_security_privacy_and_online_harms

Xue, L. (2020). *Contradictions between public perception of privacy and corporate privacy policy: A case study of TikTok*. http://summit.sfu.ca/item/20753