Click Here to Accept:
Electronic Informational Privacy on Social Media

Michael Bervell
March 29, 2019
Cambridge, MA

Submitted in partial fulfillment of the requirements for the
degree of Bachelor of Arts with Honors in Philosophy at Harvard College.

AKNOWLEDGEMENTS

In writing this thesis, I received a great deal of support and assistance.

I would first like to thank my thesis advisor, David Gray Grant, a post-doctoral fellow at Harvard, for providing me with insightful questions, revisions, thought experiments, advice, and, perhaps most nourishing, tea to drink during our many discussions of my work. You supported me greatly and were always willing to help regardless of the hour or where I was in the world.

A very special gratitude also goes to the Harvard University philosophy department for connecting me with the resources, peers, professors, and friends who encouraged me throughout the writing process. This comes with a special mention to Lidal Dror, the graduate student who patiently endured all versions (good and bad) of my ideas and writing during our weekly workshop sessions.

Third I would like to acknowledge the importance of the Embedded EthiCS program at Harvard, which provided the inspiration for this thesis. Thank you Jeff Behrends, Barbara Grosz, Jim Waldo, Cynthia Dwork, and Alison Simmons for highlighting, advocating for, and teaching the importance of ethical reasoning skills to the future computer scientists of the world, myself included.

Finally, to all of my friends and family, who provided a great deal of support in deliberating with me over the topical field of privacy on social media, as well as providing a happy distraction to rest my mind outside of my writing.

TABLE OF CONTENTS

I. INTRODUCTION

Dressed in a navy blue suit and light blue tie, Mark Zuckerberg walked into the United States Congress ready to defend Facebook before nearly 100 lawmakers from the United States House of Representatives and Senate.[1] Over the course of a 2-day hearing the 33-year-old founder and chief executive officer of Facebook answered questions about privacy, data sharing, and recent scandals. It was a media frenzy that nearly every news outlet had sent at least one reporter to cover on April 10th and 11th of 2018. As the largest social media platform in the world, Facebook was not just a pastime for the college students Zuckerberg had designed the website for: it was a worldwide cultural phenomenon.

Throughout the hearing, Zuckerberg faced almost 600 questions data privacy, data security, and consumer protection.[2] All the while, he maintained one clear belief:

> *"I believe it's important to tell people exactly how the information that they share on Facebook is going to be used. That's why, every single time you go to share something on Facebook, whether it's a photo in Facebook, or a message, every single time, there's a control right there about who you're going to be sharing it with ... and you can change that and control that in line."*[3]

It seems, as Zuckerberg alludes, that social media platforms like Facebook have an important duty to give users control of their informational privacy online. This thesis is focused on understanding and critically evaluating the claims and assumptions that Zuckerberg, other social media companies, and privacy advocates make about electronic informational privacy, its value, and the ways that social media platforms attempt to protect this privacy.

---

[1] Wichter, Zach. "2 Days, 10 Hours, 600 Questions: What Happened When Mark Zuckerberg Went to Washington." *The New York Times.* April 12, 2018.
[2] Ibid.
[3] 116th United States Congress. "Hearing Before The United States Senate Committee On The Judiciary And The United States Senate Committee On Commerce, Science And Transportation." *United States Senate.* April 10, 2018.

In chapter 2, I begin with a commonly accepted definition of informational privacy and work to provide an understanding of electronic informational privacy. By breaking the definition of informational privacy into its component parts, I define and explain phrases such as "personal information," "the ability to control," and "access" to propose a more refined definition of electronic informational privacy.

I then explore, in chapter 3, the values of electronic informational privacy when applied to the world of social media. Through the use of a thought experiment in which every social media interaction is public, I describe three values that are promoted by electronic informational privacy and lead to the living of a good life: intimacy, experiments in living, and freedom from discrimination.

Finally, in chapter 4, I conclude by investigating notice-and-consent, one of the most common forms of protecting electronic informational privacy online. Specifically, I criticize Terms of Service Contracts, the main way that social media platforms implement notice-and-consent, and propose modifications that would allow these contracts to better preserve electronic informational privacy.

With 80% of the American population using social media to communicate online every month, the phenomenon that Zuckerberg described before the United States Senate is more than a national pastime.[4] Electronic informational privacy on social media is an issue of everyday life that requires philosophical study.

[4] "Percentage of U.S. population with a social media profile from 2008 to 2019" *Statista.* March, 2019.

II. DEFINITION OF ELECTRONIC INFORMATIONAL PRIVACY

Philosophers, privacy advocates, and lawyers have constantly debated the definition of informational privacy. According to the Stanford Encyclopedia of Philosophy,

> *Informational privacy in a normative sense refers typically to a non-absolute moral right of persons to have direct or indirect control over access to (1) information about oneself, (2) situations in which others could acquire information about oneself, and (3) technology that can be used to generate, process or disseminate information about oneself.*[5]

For the sake of this paper, and as a starting point, I will simply this definition. My simplification follows what most privacy advocates consider to be a proper definition:

> ***Definition 1:*** *Informational privacy is the ability to control who has access to personal information about oneself.*

To illustrate this conception of informational privacy, let us look at a simple example. Suppose that every day I write in my diary. This diary contains deeply personal information about myself. Since I am a college student, I leave my diary in my bedroom desk drawer and expect to have privacy. Suppose a roommate of mine were to open my desk drawer and accesses the information in this diary without my permission. This action would violate my informational privacy because it would have violated my control over my personal information. Preserving my informational privacy would have required my roommate to acquire my permission before accessing my diary.

Definition 1 of informational privacy mandates that individuals have the ability to control information about themselves. What is curious about this definition is that it does not make a distinction between controls online versus offline. Thus, I argue that electronic

[5] Blaauw, Pieters, Van den Hoven, and Warnier. "Privacy and Information Technology." *Stanford Encyclopedia of Philosophy*. November 20, 2014.

informational privacy is simply informational privacy as it pertains to the Internet. Just as I wrote in my diary and stored it in my desk, I could very easily have written and stored my diary online. Moreover, just as my roommate violated my informational privacy by reading the diary in my desk without my permission, my roommate also could have violated my electronic informational privacy by reading the diary online without my permission. Electronic informational privacy, in this sense, is only distinct from traditional information privacy in its relation specifically to the online world. I will focus my writing specifically on electronic informational privacy, which I define as follows:

> ***Definition 2:*** *Electronic informational privacy is the ability to control who has access to personal information about oneself online.*

Definition 2 is a good first pass at a definition of electronic informational privacy. However, it needs to be refined in three ways. First, we need to say more about what is meant by "personal information," especially when considering the Internet. Second, we need to say more about the conditions under which a person has (and lacks) "the ability to control" who has access to their personal information. Third, properly understood, having electronic informational privacy does not just require the ability to control who has *access* to your personal information. It requires, further, the ability to control how others *use* your personal information, once they have been granted access to it. Through addressing these three concerns, I hope to propose a polished understanding of electronic informational privacy.

"Personal Information"

Definition 2 of electronic informational privacy makes use of the terms "personal information" or "information about oneself"; however, what sorts of information should be attributed to these two categories? In this section, I will strengthen and expand the view of William A. Parent to propose a definition of electronic informational privacy that clarifies

what sorts of information, when accessed, constitute a privacy violation. Ultimately, I argue that the while electronic informational privacy traditionally seems to deal with "personal information," it more adequately can be described as dealing with "personally identifiable information."

In his 1983 paper, *Privacy, Morality, and the Law*, William A. Parent argues that personal information "consists of facts which most persons in a given society choose not to reveal about themselves (except to close friends, family, etc.) or of facts about which a particular individual is acutely sensitive and which he therefore does not choose to reveal about himself."[6] For example, most persons in a given society choose not to reveal their social security number to the general public, thus Parent would describe something like a social security number as personal information. Similarly, some people in society are "acutely sensitive" to information about themselves such as their height (or weight or voice pitch). Because of this sensitivity, Parent writes, individuals may take extreme measures to ensure that other people do not find out this information. Thus, if this personal information is found out then a privacy violation has occurred. The major condition of personal information under Parent's definition is information that individuals do not want to be widely known. Thus, when this personal information is accessed a privacy violation has occurred.

Parent uses selective sharing and the sensitivity of subjects to describe the information that can create privacy violations; however, I argue that anything that can be used to identify an individual should be labeled as information that can cause privacy violations, regardless of the preferences of an individual. While Parent argues electronic informational privacy deals only with personal information, I want to expand his account by arguing that informational privacy deals with personally identifiable information. This

[6] Parent, William. "Privacy, Morality, and the Law," *Philosophy & Public Affairs.* Page 270. Autumn 1983.

personally identifiable information includes certain types of personal information that Parent's account supports as well as information that his account does not support. Similar to Parent's personal information, personally identifiable information has a relation to the habits of what most people in society only share with a few people. However, unlike Parent's personal information, the personally identifiable information I describe only relates to information that can actually be used to identify individuals, not information that individuals subjectively choose to reveal or not reveal. Electronic informational privacy, under my view, is concerned with information that can uniquely identify a particular individual. My revised definition of information privacy is external to, rather than reliant upon, the opinions of the individual.

There seem to be two motivating reasons for modifying Parent's definition of personal information as it relates to electronic informational privacy. First, it allows information that traditionally is not recognized as having the potential to violate privacy (i.e. personally identifiable information) to potentially violate privacy. Even the most mundane information, which individuals often are not sensitive to, can create a privacy violation. For instance, cellphone companies (such as AT&T, T-Mobile, and Apple) often release deidentified datasets about their users in open source research databases. These datasets may preclude information such as a name, date of birth, or address while including information such as a list of applications downloaded on a phone, a phone's Wi-Fi or Bluetooth connection history, or a phone's IP address. Under Parent's definition, the type of information included in this dataset may not be quantified as information that could create a privacy violation because it is not an instantiation of information that "most persons… choose not to reveal about them" or information that people are "acutely sensitive to."

However, by using the mundane information from these telecommunications datasets, I can understand real, personally identifiable information about an individual, such as whom he/she is similar to (via phone application downloads); what sorts of car he/she drives (via previously connected Wi-Fi/Bluetooth networks); or where he/she lives (via IP addresses). This, what I call the problem of mundane inference, allows for seemingly impersonal information to become extremely identifiable to an individual, their preferences, or their personality. While Parent would argue that accessing this information should not constitute a privacy violation because it is not "personal information", I argue that because this information is personally identifiable information it should constitute a privacy violation if accessed improperly.

The second implication of viewing informational privacy as personally identifiable information is that it challenges Parent's argument that informational privacy is dependent upon subjective sensitivities. Parent argues that any extreme sensitivity can be personal information (e.g. if I am extremely sensitive about my height, my height can be called personal information). The implication of his argument is that any information can be personal information, if an individual is sensitive enough, and can cause a privacy violation. I argue, instead, that personally identifiable information, which is not concerned with how sensitive an individual is, should be the standard for information that can create a privacy violation.[7] For example, suppose I am very sensitive to people knowing that I am going bald and, as a result, I wear a hat every single day so people do not know that I am going bald. Parent would argue that the fact I am going bald is "personal information" and discovering that fact would be a violation of my privacy. However, I would argue that discovering my

[7] Under this view, even if an individual were extremely sensitive to information about himself or herself, this by itself would not constitute potentially privacy-violating information. Instead, only information that could uniquely identify an individual could be called potentially privacy-violating information.

baldness would not violate my privacy because there is nothing private about the information. While discovering my baldness may violate another value of mine, such as the right not to be embarrassed, it does not seem to be a privacy violation because it is not uniquely identifiable information. About 750 million people in the world (10%) are bald.[8] While the fact that I am bald is deeply personal, there is no privacy violation in accessing only this information because it is not uniquely identifiable or specific to me. Suppose further, however, that I lived in a community where baldness was a uniquely identifiable trait. If this were the case then discovering my baldness could constitute a privacy violation because baldness links itself back to me, and only me, in this community. Ultimately, sensitivities should not be used to define the information in informational privacy; instead it should be personally identifiable information.

We can raise a distinction here between personally identifiable information and identifying information. While identifying information is any information that can identify an individual, personally identifiable information is that information which can practically be used to identify a specific individual. For instance, suppose that I have my social security number written on a card and give it to my brother. To him, this informational is both identifying (any social security number is identifying) and identifiable (he can link this information to me specifically). However, suppose that my brother were to drop this social security card while traveling in another country and a stranger ere to pick it up. If this card did not describe the type of information on it, all this stranger would see is a sequence of 9 number numbers and, though these numbers may be identifying information, the numbers would not be identifiable because it could not be used by itself to identify me. The ability to

[8] "How Many Bald People Live on Earth?" *Quora*. December 14, 2017.

link information to a specific individual, in this sense, is the prerequisite for defining "personally identifiable information."

I revise the definition of electronic informational privacy to be one that does not deal with personal information, but instead deals with personally identifiable information since it seems this information is the type of information that constitutes privacy violations. In short, personally identifiable information consists of uniquely identifying facts that persons in a given society choose not to reveal about themselves (except to close friends, family, etc.).

> ***Definition 3:*** *Electronic informational privacy is the ability to control who has access to personally identifiable information about oneself online.*

In light of definition 3, many would argue that personally identifiable information should not be the metric for defining electronic informational privacy because identifiability and privacy seem too distinct. For instance, suppose that I am a collegiate athlete showering and changing in my team's locker room after practice with my team. Unbeknownst to the rest of my team and me, a camera is live-streaming this information to televisions across the world with very low camera and audio quality. Quality so low that nobody (myself and my team included) can identify the locker room, the people in the video, or any other identifiable facts. Would accessing this video be an informational privacy violation?

Yes, the video contains deeply private information of my teammates and me (information that Parent would argue is personal information because of our sensitivities to nudity); however, I argue that accessing this video would not be an informational privacy violation. This is because privacy violations do not deal with the information itself, but in the identification of this information to a specific individual. If no one is able to say that I am the person in the video or that my team is the team in the video then accessing this video invades no ones privacy. However, if the video contained any information that could potentially

identify my teammates or me, then accessing this video would undoubtedly constitute a privacy violation. But, for this privacy violation to occur there must be a way to identify the people in the video.

Another argument in response to definition 3 is that not all personally identifiable information seems to be the types of facts that would constitute a privacy violation. Consider the fact that Elizabeth Warren is the only female Senator of Massachusetts. This information is a uniquely identifiable fact about Warren; however, if we accessed this information we would certainly not call it a privacy violation. In response to the Elizabeth Warren counterexample, I concede that accessing this information would not constitute a privacy violation. However, this is not because of the information itself, but instead because of controls related to this information. Since this information was released in accordance to the law, accessing it does not constitute a privacy violation. It seems, then, that there are social norms that constitute what personally identifiable information does and does not constitute electronic informational privacy violations. For example, around the world nudity is seen as personally identifiable information; however, there are social contexts (e.g. spas or nude beaches) where this norm is suspended in public. I will discuss this nuance more in the next section when I clarify the phrase "the ability to control."

Potentially privacy-violating information should be related to identifiable and unique facts about an individual that is not widely shared, regardless of their sensitivities to this information. What Parent's account misses is the fact that basing personal information on subjective opinions does not actually have any bearing on what is or is not potentially privacy-violating information. Potentially privacy-violating information is that which can be used to uniquely set one individual apart from another.

"The ability to control"

To understand the phrase "the ability to control," I will first describe the view of Helen Nissenbaum. Her view provides a way of understanding what sorts of control constitute electronic informational privacy. Then, I will use this understanding to refine Definition 3 of electronic informational privacy. Ultimately, I will argue that "the ability to control" can be simplified to "the following of rules" about personally identifiable information.

In her 2009 book *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Helen Nissenbaum gives an account of privacy in terms of "expected flows of… [personally identifiable] information."[9] Nissenbaum's flows are composed of actors (e.g. subject, sender, recipient), attributes (types of information), and transmission principles (constraints under which information flows). For example, in the healthcare context patients expect their physicians to keep personal medical information confidential, but patients also accept that this information can be shared with specialists as needed without asking explicitly for their permission.[10] If a physician breaches patients' expectations by selling this information to a marketing company then, Nissenbaum writes, informational norms for the healthcare context would have been violated. When the flow of information adheres to the entrenched and expected norms of a context then all is well. However, if the flow of personally identifiable information does not follow expected norms then a privacy violation has occurred.

[9] Nissenbaum, Helen. "Privacy in Context: Technology, Policy, and the Integrity of Social Life." *Stanford University Press*. November 24, 2009.

[10] In this example, the actors are the healthcare patients, physicians, specialists, and marketing company; attributes are confidential medical information; and constraints are that set out by law in the Health Information Privacy and Protection Act (HIPPA) as well as other health care laws.

Using Nissebaum's logic, I argue that "to control" personally identifiable information is to have every expected actor that comes into contact with ones personally identifiable information follow the rules associated with that personally identifiable information. If an expected or unexpected agent ever "breaks" the rules associated with this information then a privacy violation has occurred. This theory is especially practical in our current era of massive information sharing and complex information flows. It redefines privacy violations in terms of principles that deal with information itself rather than with the individuals from whom the information has come from. As a consequence, the judgment of what constitutes a privacy violation is framed in terms of privacy-protecting rules rather than individual control. These information-specific privacy-protecting rules seem to come from two major sources, social norms and voluntary agreements.

The first source of privacy-protecting rules is social norms, informal understandings that govern the behavior of members of a society. These social norms may be enforced by the law (which enhances good social norms while undermining bad ones) or by unspoken social pressure from other members of a society. In context, some of these social norms also happen to deal with electronic informational privacy. For example, suppose I seek to write a private SMS (short message service) text message on my iPhone to send to my mother, assuring her that I am faring well in college. After sending the message, my mother subsequently shares this information with my father even though I did not explicitly give her permissions to do so. In such a scenario, her choice to expand access to my personally identifiable information may not constitute a privacy violation because it falls in line with rules defined by social norms. These norms, which I did not create but are laden in the habits of society at large, would imply that information could be freely shared between members of a family without

violating privacy. However, if my mother shared this SMS text message with a newspaper we would be inclined to argue that by doing so she has violated my electronic informational privacy. The reason being that there is no social norm (and presumably no other privacy-protecting rules) that support my mother's decision to share my private information with a newspaper.

As expected, privacy-protecting rules may differ from culture to culture because social norms may differ from culture to culture. For instance, since 1814 Norwegians have been able to see how much everyone else in their country earns and pays in taxes. In 2001, this information was placed online and searchable in a database for anyone with a Norwegian national ID.[11] While disclosing the salary of your neighbor on Facebook may violate electronic informational privacy norms in the United States, this same action would not violate electronic information privacy norms in Norway because of vastly different social norms. The expectation of privacy enforced by social norms, then, is directly related to the society at large.

The second source of privacy-protecting rules is voluntary agreements. These agreements are voluntarily entered into by multiple parties and can be explicitly or implicitly stated. Traditionally, voluntary agreements are enforceable by law (when written and signed) or by one of the parties who entered into an agreement. One great example of voluntary agreements are the terms of service contracts that online social media companies require their users to sign. These agreements are all-or-nothing contracts that corporations require users of a product to agree to in exchange for service. They define what expectations of privacy individuals can have while using a given service and explicitly state these expectations. If a corporation violates this voluntary agreement then a privacy violation has occurred and the

[11] Bevanger, Lars. "Norway: The country where no salaries are secret," *BBC*. July 22, 2017.

platform user can use the law to ensure that these harms are repaired. I will discuss terms of service contracts in more details in chapter 3.

Another example of a voluntary agreement is a verbal contract made between two parties. For instance, suppose I am leading a vulnerable discussion amongst a student-group that I am part of. I may institute a "four-wall policy" for everyone at the meeting, stating that what is said in the room should not leave the room. While there is no law to enforce this, through creating a verbal agreement with everyone in the room I have crafted a privacy-protecting rule that I expect meeting attendees to follow. If these attendees ever break the voluntary agreement of four-wall policy then a privacy violation has occurred.

It is also worth noting here that various rules can apply to the same piece of personally identifiable information; however, regardless of what combination of rules apply to this information, I define electronic informational privacy as the preservation of rules at *all* points of contact for this information. For instance, in the scenario where I decide to write an SMS text message to my mother there are more actors than just my mother and myself. First, I transfer information from the private location of my mind to the public location of my iPhone SMS message box. Then, I send this message from my personal device to a nearby cell phone tower or control channel. Generally this process runs on the backbone of the Internet, a "packet-based" approach often referred to as TCP/IP (transmission control protocol/Internet protocol). The "packet" that is sent through the network not only contains my SMS message, but also other personally identifiable information such as the phone number of my device, the length of the message, the message format, the time stamp, the destination, and more. After the message is sent, it moves from tower to tower until reaching

its destination, my mother's phone. Finally, my mother reads the SMS message and my private information is shared with her.

This scenario, which seemed only to include my mother and myself, actually involves dozens of actors – physical and digital, living and non-living, algorithmic and non-algorithmic. However, these actors all serve to promote my interest of communicating with my mother through following social rules and voluntary agreements. If at any point of this process an actor violated the rules associated with my information, then I would claim that an electronic informational privacy violation has occurred.

These instantiations of privacy-preserving rules are examples of expectations of privacy that govern the exchange of information. To "control" informational privacy is simply to maintain the expectations of privacy laden in these rules. Thus, I revise the definition of information privacy to be as follows:

> ***Definition 4:*** *Electronic informational privacy is the following of rules about access to personally identifiable information about oneself online.*

"Access to"

Our definition of electronic informational privacy still seems to be lacking because it only deals with access to personally identifiable information and not use of this personally identifiable information. In addition to being required to follow rules about who has access to uniquely identifying facts about you, individuals should also have the right to enforce rules about the use of these facts. In this sense, even if the way that someone accesses personally identifiable information does not constitute an electronic informational privacy violation, the way someone uses this information can constitute an electronic informational privacy violation. Use-based privacy violations can occur if information given with a set of expectations is not properly respected. Similar to the rules that apply to *accessing*

information, there are rules that apply to *using* this information. Social norms and voluntary agreements are two examples of the types of rules that can govern proper use. Thus, if one's information is used in a way that does not follow these rules, an electronic informational privacy violation has occurred.

It is worth explaining briefly what sorts of rules exist in relation to the use of uniquely identifying facts about an individual. First, there are social norms that instantiate themselves in the form of laws to prevent people from being improperly manipulated by the use of their information. One such example is the Civil Rights Act of 1964, which has many anti-discrimination provisions such as Title VIII that provides equal employment opportunities and "prohibits employment discrimination based on race, color, religion, sex, and national origin."[12] The law quite clearly states that in America, certain forms of using information in order to discriminate should not be allowed. I argue, further, that if information is used against an individual in this way then an electronic informational privacy violation has occurred. In such a scenario, the use of personally identifiable information, not the access to it, creates a privacy violation.

These social norms need not be instantiated in the law to be meaningful: they could be implied by the social context at large. For instance, suppose that Jonas is a pre-med student who is very close with the dean of a medical school he would like to apply to. During a dinner that Jonas has with this dean, he reveals to the dean in confidence that he has recently been diagnosed with HIV/AIDS. Months later Jonas, the stellar medical school applicant, is interviewed to become a heart surgeon and wows the admission committee. While deliberating about Jonas' admission status, the dean ultimately decides that even though Jonas is extremely qualified and otherwise would have been accepted, they will not

[12] The 88th United States Congress. "Civil Rights Act of 1964." July 2, 1964.

admit him to medical school because of his condition, despite the fact that the dean learned this information in confidence.[13] In this scenario even if, there were no laws preventing this personally identifiable information about Jonas' health from being a consideration in his application, we would still like to say that a privacy violation would occur if the dean used this personally identifiable information about Jonas to weaken his admission status. Since Jonas voluntary shared this information with the dean in confidence and without the knowledge that the information could be used in relation to his acceptance to medical school, there are no social norms that grant the dean the right to use this information as a factor in his application. Determining if an information privacy violation has occurred would require us to determining the rules associated with the use of information rather than access to information. Since, generally, a social norm may be that information told in confidence should always remain in confidence, I argue that by using this private information in a way that undermined Jonas' application, the dean violated Jonas' informational privacy.

Second, there are electronic informational privacy use-violations that result from not following rules created by voluntary agreements. For example, in the 2016 presidential election, Facebook played a large role in influencing voters through influential, individual-specific advertisements. Firms, such as Cambridge Analytica, created these targeted advertisements through applying algorithms to data from Facebook users' online profiles. Arguably, both Facebook and Cambridge Analytica properly accessed the data and did not violate any users' informational privacy when curating these datasets because users agreed to terms of service contracts before sharing their data. However, after properly accessing this

[13] It is important to note here that this example specifically describes a *use* violation of informational privacy and not an *access* violation of informational privacy. If the dean, for instance, were to share this information with the admissions committee rather than single-handedly rejecting Jonas, then one could argue that the committees' access to Jonas' information was what led to the privacy violation. This example, however, is focused on the use, and more specifically the improper use, of Jonas' personally identifiable information.

Facebook data, Cambridge Analytica *use* these vast troves of permanent, identifiable facts about individuals to influence in ways that violated electronic informational privacy. While there was nothing explicitly barring Cambridge Analytica from using data to create advertisements, I would argue that the scope of this use (i.e creating psychological profiles of users for political manipulation) far overstepped Facebook's terms of service contract. Casting this specific case aside, the point I hope to make is that while individuals may accept to a platform's access-based terms of service and institutions may follow these terms, it is still possible for electronic informational privacy violations to occur as a result of use. In light of predictive privacy harms that exist in the era of big data, machine learning, and algorithms it is important to consider use and not only access in defining informational privacy.

Since the use of personally identifiable information about an individual can constitute an informational privacy violation, I revise the definition one final time to be as follows:

> ***Definition 5:*** *Electronic informational privacy is the following of rules about access to and use of personally identifiable information about oneself online.*

Ultimately, the definition that I provide for electronic informational privacy is one that allows for and even mandates control of information by the individual online. This information, personally identifiable information, must be properly accessed or used in accordance to rules in order to avoid violating electronic informational privacy. As I continue discussions of electronic informational privacy in my next two chapters, I will explore why this definition is valuable as well as how social media platforms have attempted to protect it. While not explicitly mentioned, I note here, that many of the values and consequences that I discuss will also apply to the offline world of traditional informational privacy.

III. VALUE OF ELECTRONIC INFORMATIONAL PRIVACY

Individuals seem to have preferences about what is public and what is private. For instance, many would like there to be a boundary between who knows what happens in the house (private) versus what happens outside of the house (public). Similarly, nearly all would expect a separation between what happens in my head (private) and what happens in the world (public). As I argued in Chapter 1, these preferences also manifest themselves in the online and digital world. For some reason, many prefer that just as their diaries are private their emails be private as well and just as their name is public their LinkedIn profile is public as well. Perhaps the desire for this separation of public and private comes because people find value in both informational privacy and electronic information privacy. Both forms of privacy seem to allow individuals the opportunity to escape the gaze of the public and be their true selves. Moreover, it seems that without these forms of privacy certain values that facilitate the living of a good life (such as the right to be free from discrimination or ability to create intimate relationships) would be undermined. To this observation, I seek in this chapter to answer one question: Why is electronic informational privacy ("the following of rules about access to and use of personally identifiable information about oneself online") valuable?

While I provided a definition of electronic informational privacy in Chapter 1, I have not yet explained why it is valuable. In this chapter, I will argue that the reason why people have preferences for electronic informational privacy is because electronic informational privacy is valuable. Specifically, I find that electronic informational privacy is valuable because it is the catalyst that allows for other values to exist. Throughout this chapter, I will use "social media" as a concrete, online example to help ground my abstract arguments about

electronic informational privacy. Social media is a particularly useful case study to explore because over 3 billion people around the world use it every day to communicate with one another and understand the world.[14] In using social media, these individuals from all walks of life share massive troves of personally identifiable information with social media companies. Thus, almost half of the world's population has entrusted the companies that run social media platforms with protecting their electronic informational privacy and users expect to have control over their data. Social media is possibly the best lens towards understanding examples of the value of electronic informational privacy.

To begin my exploration of the value of electronic informational privacy, I will first describe what exactly "social media" is and make the case for why protecting privacy on social media, as opposed to traditional media, is particularly important. Then, I will defend why electronic informational privacy is necessary for intimacy, facilitates experiments in living, and prevents certain forms of discrimination – especially when applied to the realm of electronic informational privacy on social media. Each of these values is uniquely worth promoting, but all rely upon electronic informational privacy. Throughout these sections, I will use the values I described to explain the potential electronic informational privacy harms of social media.

What is Social Media

Social Media platforms, quite simply, are online websites and applications that enable users to create and share content or to participate in social networking. Some of the most popular Social Media sites today include Facebook (valued at $484 billion), LinkedIn (valued at over $26 billion), WhatsApp (a subsidiary of Facebook), Instagram (a subsidiary

[14] "Number of social media users worldwide from 2010 to 2021 (in billions)." *Statista.* July, 2017.

of Facebook), Twitter (valued at $23 billion), Snapchat (valued at $12 billion), Reddit (valued at $3 billion), and YouTube (valued at $160 billion, and a subsidiary of Google).[15] These eight social media sites are the most used; however, there are even more platforms online. On most of these platforms, users are incentivized to upload information about themselves and connect with peers that they interact with in life. In this sense, social media sites provide a digital mirror of an individual's personality or network from the real world.

For users, many of these social media platforms are free to use; however, in order to make money the companies that create social media platforms turn to a few techniques. As the common adage goes, if you're not paying for the product, the product is you. Generally, social media platforms generate revenue by commoditizing users: they provide access to platform users (through advertising), offer exclusive services to users (through premium upgrades or content), or sell information about users (through third-party data brokering).[16] In fact, social media platforms have even created a metric for understanding how efficiently they are commoditizing their users, annual revenue per user (ARPU). Facebook, for example, reported in its 2017 SEC annual report that its average ARPU was $20.21.[17] This means that its 1.74 billions users brought it over $35 billion of revenue. Similarly, Twitter in its SEC Registration statement described the importance the advertising, premium upgrades, and data brokering:

> *Our ability to increase the size and engagement of our user base, attract advertisers and platform partners and generate revenue will depend in part on our ability to improve existing products and services and create successful new products and services, both independently and in conjunction with third parties.*[18]

[15] Kerby, Justin. "Here's How Much Facebook, Snapchat, and Other Major Social Networks are Worth." *Social Media Today*. May 16, 2017.
[16] Campbell, Steve. "How do Social Networks Make Money?" *Make Use Of.* April 30, 2010.
[17] United States. Securities and Exchange Commission. *Facebook: Form 10-Q.* 31 December 2017.
[18] United States. Securities and Exchange Commission. *Twitter: Form 10-Q.* 31 December 2017.

By having a larger and more engaged user base, Twitter is able to satisfy shareholders by providing a variety of services that generate revenue. Though these are just two examples, the commoditization of users is inexplicably tied to the success of nearly all social media platforms.

User generated content, sharing, and consumption is also central to many social media platforms. This content is displayed to users in a user-specific news feed that, using algorithms, displays the most relevant content to users based on their previous interactions with the platform. For instance, Instagram features a newsfeed that is primarily composed of photos from the individuals that a user "follows." Thus, nearly every Instagram user has a unique newsfeed that is curated with content that they are interested in consuming based on their preferences. Similar feeds are used on Facebook, LinkedIn, and YouTube to keep users coming back to the platform as often as possible. Additionally, social media platforms encourage users to consume content that they otherwise would not be exposed to. For instance, Instagram encourages users to browse an "Instagram Explore" section of the app which features publically posted content for users to consume even though their friends have not posted it. Similarly, Snapchat's "Discover" feature rotates daily and has become an online instance of the tabloid newspapers and gossip magazines that tell scandalous stories about celebrities.[19]

Social media platforms, in their technical capabilities, are vastly different from the nearest traditional media sources, newspaper and television. Despite this difference, the general public has widely adopted social media with over 3 billion people around the world

[19] Read, Ash. "The News Feed is Outdated: How Stories Changed the Way I Think About Social Media." *Buffer*. November 16, 2018.

and 77% of Americans using it.[20] However, the importance of social media stretches beyond the numbers. Social media is particularly relevant to electronic informational privacy because it raises powerful privacy concerns that are distinct from those of traditional media. Throughout the remainder of this chapter, I will use the example of social media to describe the value of electronic informational privacy.

Billboard State Thought Experiment

To demonstrate the value of electronic information privacy I will be focusing on a central thought experiment: "The Billboard State Thought Experiment." As a child, my parents always told me to act as though everything I was doing would be projected onto a billboard for all to see. Whether I was by myself in my room or interacting with my classmates, I always thought to myself "would I want everything I am doing to be shown to the world?" In the Billboard State, everything that anyone does is public for free access and use. In the Billboard State, there is no public/private distinction; everything that would traditionally be thought of as private is available as public.

While the Billboard State was a technique my parents used to instill integrity in me at an early age, we can imagine that an online version of this thought experiment can shed light onto the value of electronic informational privacy. Suppose that in the Billboard State everything that anyone does on a social media platform (e.g. Facebook, Twitter, or Instragram) is public. Every interaction that users have with social media platforms is public for anyone to read, copy, and distribute. This includes all inbound messages, posts, photos, and outbound messages along with information about when you log in, how long you log in for, and everything else that is traditionally part of the "back-end" of a social media profile.

[20] "Number of social media users worldwide from 2010 to 2021 (in billions)." *Statista.* July, 2017.

Moreover, in the Billboard State for the foreseeable future every interaction had with a social media platform will also be public. As a result of this constant monitoring what you assumed was private is perpetually revealed, in its most raw form, to the public. The Billboard State is a world where there is no electronic informational privacy on social media.[21]

Defending Privacy's Value on Social Media

While the Internet creates a "digital persona" that is different in body from one's actual personality, I argue that online electronic profiles are very revealing about an individual's mind and the true nature of an individual. Thus, in making all actions on and related to social media public, I argue that this will actually have an effect on how people live their lives in the world. The Billboard State, which effectively eliminates electronic informational privacy on social media, would have many consequences; however, I will only discuss three in this section. First, people would not be able to create beneficial intimate relationships through social media because electronic informational privacy is what allows these relationships to exist. Second, individuals will not be able to participate in experiments of living that lead to the development of the self. Third, individuals would be subject to discrimination in advertising that could arise through the use of personally identifiable information that would otherwise be private under the traditional rules of electronic informational privacy. Through exploring the consequences of the Billboard State thought experiment, I hope to defend the values of electronic informational privacy.

[21] Perhaps social media is not where you most desire electronic informational privacy. If this is the case, suppose that some other online part of your life is made public by the rules of the Billboard State. All of your text messages, actions with your Amazon Alexa, emails, or phone conversations are revealed publically and you can do nothing to stop it.

Preserving Intimacy

One of the values that electronic informational privacy protects, and the reason why electronic informational privacy is valuable, is that it creates space for intimacy. In this section, I will use the philosophical arguments of Charles Fried and James Rachels to argue that in the absence of electronic informational privacy there would be little to no intimacy. This will be evidenced through the example of the Billboard State.

In his 1968 paper *Privacy*, Fried argues that privacy is essential for relationships such as love, friendship, and trust.[22] He writes that intimacy relies on the voluntarily sharing of information about one's actions, beliefs, or emotions with another. Since there is no obligation to share this information, when an individual chooses to reveal information (i.e. to be intimate) they are choosing to provide a unique insight about himself or herself to the person that they are sharing this information with. What makes this relationship "intimate" is the fact that this information, which did not need to be shared with anyone, was freely shared with someone. Privacy is what allows information to be shared with distinct people in distinct amounts.

Informational privacy is what allows us to have varying relationships with various people, each of whom knows different amounts of information about us.[23] As James Rachels puts the point in his 1975 paper *Why Privacy is Important* "privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have, and that is why it is important to us."[24]

---

[22] Fried, Charles. "Privacy," *Yale Law Journal*. 1968.

[23] To see this point more clearly, consider what happens when two close friends or two spouses are joined by a casual acquaintance. Undoubtedly, the character of the group changes: the close friends will opt to discuss different issues than if a stranger were not present and the partners will put on a "public" face that isn't apparent when the third-party is not there.

[24] Rachels, James. "Why Privacy Is Important." *Princeton University Press*. 1975.

Perhaps the best way to see this is to consider what would happen if we did not have the ability to discern between what information was and was not shared with certain individuals. Suppose that every fact about your actions, beliefs, or emotions was shared with everyone. In such a scenario, there would be no difference between "casual acquaintances" and "intimate acquaintances" because all individuals would know all information about you.[25] The expectation of informational privacy, quite necessarily, facilitates the development of differing levels of friendships and intimacies. The ability to have these differing levels of friendship ultimately increases our quality of life by allowing us to develop various interpersonal friendships that provide us fulfillment in life as social-animals in need of relationships. These interpersonal relationships can bring pleasure and joy to people involved in them and, as some scientific studies have found, are even positively correlated with outcomes such as longevity and health.[26] Without privacy, there would be no intimate relationships to better allow us to live a good life.

Referring back to the Billboard State, let us infer what may happen to our various intimate relationships if everything that dealt with social media were public. Consider Instagram, a photo-sharing social media platform. Many users of Instagram have both a real Instagram account where they craft a public self and a fake Instagram account, or Finstagram account, where they can "post ugly selfies, private jokes, personal rants, pictures of outfits

---

Rachels also continues by writing "By a 'social relationship' I do not mean anything especially unusual or technical; I mean the sort of thing which we usually have in mind when we say of two people that they are friends or that they are husband and wife or that one is the other's employer."

[25] One could potentially argue that *emotional engagement* (i.e. time spent with a partner) is what truly creates intimacy with another individual, not the amount of unique information shared. For example, the argument goes, if a couple were on a honeymoon they would develop intimacy regardless of what they choose to share with one another because they are spending time with together and making unique memories that only the two of them have. However, I argue that this engagement would only create memories that are meaningful because these memories private. That is to say, the memories are only shared between you and the individual(s) with whom you had the experience. In reality there is no difference between an intimate memory like this and information that I selectively choose to share by speaking. Without any informational privacy, intimate memories, which can also develop intimate relationships, would also be public.

[26] Vaillant, George. "Triumphs of Experience: The Men of the Harvard Grant Study." *Belknap Press*. 2012.

you're genuinely seeking advice on, screenshots of funny family group texts, pictures of yourself in the middle of a good cry, that sort of thing, to a relatively sympathetic audience."[27] Traditionally while an Instagram account may have hundreds or thousands of public followers, a Finstagram account is a private account that only a handful of true friends as followers. These accounts, which rely on electronic informational privacy to exist, mimic the desire in the offline world to develop varying relationships through information sharing. Finstagrams function by allowing users to choose who will be able to see certain information about themselves because they require users to approve followers rather than making the ability to be followed public. As such, these accounts limit the sharing of information to a handpicked group. The members of this group (the followers of a Finstagram) thus have a more intimate relationship than those individuals who follow the same individual's traditional and publically available Instagram account.

In the Billboard State (which eliminates electronic informational privacy) everything on Finstagram accounts would be public and Instagram users would be unable to use social media as a means of creating varying levels of intimacy. Users would be forced to present every post to the whole world instead of limiting the posts to a group of handpicked followers. As a result, there would be no difference between "intimate" friends on Instragram and "casual" friends on Instagram. Essentially, all friendships on Instagram would be one and the same. Instagram would no longer be a platform that could create differing levels of friendship through information sharing. As I argued before, without this ability to create intimate relationships online, people would not be able to lead fully fulfilled lives because this requires intimacy through interpersonal friendships.

[27] "Finstagram – a secret Instagram account to post ugly selfie," *The Guardian*. February 21, 2017.

As evidenced by Rachels and Fried, in the Billboard State, and in reality, electronic informational privacy on social media is valuable in that it creates the space intimacy, which allows individuals to live the good life. If there were no electronic informational privacy then people would not be able to develop varying levels of relations with people online or offline. Electronic information privacy is necessary in creating various levels of relationships and results in a myriad of benefits for those involved in the relationship.

Permitting Experiments in Living

Electronic informational privacy also permits the value of what John Stuart Mill called "experiments in living" that allows for the development of the individual. In this section, I will use the arguments made by John Stuart Mill in addition to the Billboard State to defend how and why experiments in living are promoted by electronic informational privacy. Then, I will describe why experiments in living are important through describing how they facilitate development.

In Book III of *On Liberty*, J. S. Mill describes "experiments in living" as the ability to test different types of characters and lifestyles in order to discover conceptions of the good for ourselves.[28] Mill rejected the traditional view of his time that people know about the good through a priori intuitions and instead argued that as long as experiments did not create injury to others, "the worth of different modes of life should be proved practically." He recognized that mankind is imperfect and fallible, as such the truths that we recognize as fact still need to be tested through life experience instead of being blindly believed. Mill continues to argue that one of the reasons why people are unable to practice experiments in living is because of the "tyranny of public opinion." Unlike the interference of the State in public affairs, the social opprobrium of public opinion enforces conformity and stifles individuality through

[28] Mill, John Stuart. "On Liberty." *Longmans, Green, Reader and Dyer*. 1859.

social pressure and scorn from the majority. If people become too scared to act in ways that break orthodox because of social consequences, then this would become a huge limit on the development of individuality and lead to what Mill calls the enslaving of the soul. For these reasons, Mill argues that everyone must protect the freedom to express themselves especially in ways that do not seem to fit the norm for the sake of individuality and social progress.

To understand this Millian idea, let us put it to the test. Suppose that a child were curious as to whether or not they wanted to wear high heels. Understandably, even though this child has seen adults in their life wearing such shoes, they may not know if this action would be good for themselves. One day this child wears high heels to school and, after a day of experiments in living, decides that high heels are for them. If this child were a girl, there would be no need to protect them from the tyranny of public opinion since the majority group that wears high heels is female. Nonetheless, Mill would argue that this girl would have discovered a truth about herself. However, if this child were a boy then the tyranny of public opinion could manifest itself in the patronizing opinions of his classmates, teachers, or community. Thus, if a boy never experimented with wearing high heels for fear of social consequences or if the boy was forced to retreat from this experiment because of social censure then there would be a limit on his development of individuality and his ability to discover the good for himself. Mill, in such a scenario, would claim that in not allowing the boy to experiment in living, we are stifling the development of his individuality regardless of what the "norm" or the majority describes. The value of experiments of living is that they give individuals the opportunity to explore the self in order to become more enlightened about what the good is for themselves.

Privacy is valuable for conferring experiments of living because it enables free experimentation without actors having to be concerned with what the majority might say about them. In the previous example, we assumed that a child would venture into the public to engage in an experiment of living. However, it is also conceivable that a boy or a girl would simply wear high heels within the privacy of their own home in order to discover what is good themselves. In such a scenario, privacy would protect this child from the tyranny of public opinion that could stifle individual development. Privacy enables free experimentation without the worry of public opinion.

I argue that experiments in living also manifest themselves online and, as I hope to show in the Billboard State, electronic informational privacy helps to enable experiments in living online. This benefit is that electronic informational privacy allows individuals to use the vast resources of the Internet for self-exploration and self-enlightenment as to what constitutes the good for them, without fear of these experiments negatively harming them in the future.

Suppose that in the Billboard State I decide to browse various pages of alt-right or alt-left celebrities for the sake of my own curiosity, self-development, and wrestling of different opinions. Since in the Billboard State everything is public, my browsing history will be open for scrutiny to anyone who would like to see it. Later in life, I decide to run for public office in the Billboard State and this radical browsing history is brought to light as an example of my radical character. We can imagine that in such a scenario, the public would be in uproar and the tyranny of public opinion would have a negative impact on my overall campaign. In a world that lacks electronic informational privacy, any experiment in living that is undertaken in favor of self-development could be used against the individual experimenting,

especially if this experiment does not fall in line with public opinion. This tyranny, subsequently, would result in a scenario where individuals are incentivized not to freely experiment in living, but instead to simply fit into the norm to avoid social ostracization.

Electronic informational privacy is linked to experiments in living because this privacy protects individuals from the judgmental gaze of the majority. This privacy-induced protection is important because it permits individuals to explore unpopular opinions that, though controversial, can develop an individual's mindset and outlook on the world. The fact that an opinion is unpopular does not automatically render it incorrect; however, in the Billboard State there would be no incentive to wrestle with or explore unpopular opinions because the negative consequences of public opinion would outweigh the benefits of individual development. Thus, in the absence of any electronic informational privacy individuals would experience less intellectual and character development because they would be dissuaded from conducting experiments in living.

Outside of the Billboard State, we have seen the benefits that can be associated with allowing individual experimentation online as a form of development. One clear example of this is the rise of online social media communities that allow marginalized LGBTQ youth the ability to have a safe space for expressing and exploring issues of sexuality and gender that would be ridiculed in their physical communities. In her 2017 paper, Leanna Lucero describes how private Facebook groups help marginalized LGBTQ youth by allowing them to "safely navigate their lives through learning, participating, engaging, communicating and constructing identities in digital spaces."[29] Without electronic informational privacy (in this case the right to exist privately in a group where your membership is not known) these youth

[29] Lucero, Leanna. "Safe spaces in online places: social media and LGBTQ youth." *Multicultural Education Review.* April 12, 2017.

would not have the safety to explore their unpopular identity while also being free from the judgment of the majority. Moreover, on platforms such as Reddit, electronic informational privacy allows individuals anonymity that would not be possible in the physical world.[30] This anonymity, as with membership of a private group, provides the space for the "developmentally and culturally appropriate venue for the exploration and subsequent commitment to an integrated sexual orientation identity."[31]

The prevalence of these experimentation communities also extends beyond the LGBTQ communities. For instance, in in 2001, the Pew Research Center reported that nearly 80% of Internet users participated in online groups to help others by sharing information and experiences.[32] Since the rise and proliferation of social media this number has only increased. Presumably, just as members of the LGBTQ found communities that allowed for experiments of living, any Internet user could find communities to contribute to their intellectual or lifestyle development. Ultimately, the expectation of electronic informational privacy is what allows for the protected development of these individuals through experiments in living. Electronic informational privacy on social media shields people from the tyranny of public opinion and instead allows for experiments in living online that develop an individual by limiting who has the ability to view an individual's experiments.

Electronic informational privacy is what allows social media to be a place for the development of individuals through experiments of living. Because the tyranny of the

---

[30] Harper, Gary. "The Internet's Multiple Roles in Facilitating the Sexual Orientation Identity Development of Gay and Bisexual Male Adolescents." *American Journal of Men's Health.* January 13, 2015.
[31] Gary W. Harper continued to describe just a few of the other benefits that anonymous self-exploration has provided LGBTQ youth. These youth "reported that the Internet provided a range of functions with regard to the exploration and acceptance of their sexual orientation identity, including: 1) increasing self awareness of sexual orientation identity; 2) learning about gay/bisexual community life; 3) communicating with other gay/bisexual people; 4) meeting other gay/bisexual people; 5) finding comfort and acceptance with sexual orientation; and 6) facilitating the coming out process."
[32] Horrigan, John. "Online Communities." *Pew Research Center.* October 31, 2001.

majority can stifle individual development (and lead to what Mills calls the enslaving of the soul) it is important that these practical experiments for self-discovery online are protected by electronic informational privacy.

Preventing Discrimination

Another reason that electronic informational privacy is important is because it prevents some forms of discrimination against individuals. In this section, I will use the example of social media advertising and the Billboard State to argue that freedom from certain types of discrimination is a direct consequence of electronic informational privacy.

To begin, it is worth understanding the sorts of discrimination that can be created through using social media platforms. Traditionally, online advertisers on social media platforms facilitate these forms of discrimination. Online advertising, as a result of social media platforms, has become much more effective and popular for advertisers because it is much more targeted and more effective than traditional media advertising. Since social media platforms incentivize users to submit factual information about themselves, these platforms have an accurate insight into their users' real-world experience. These platforms then provide advertisers with a unique ability to target advertising for specific subsets of users. In 2017 alone, worldwide investments in social media advertising clocked in at over $32 billion and Internet media advertising spending was around $200 billion.[33] These advertisers ranged from politicians to media moguls, but all shared in their desire to utilize information provided by users online to influence them directly. Unlike advertising in newspapers or on television, social media advertising is unique in its specificity and cheap costs. Suppose that I were the Chief Marketing Officer of Coca-Cola in 1919. If I wanted to market to Americans to drink

[33] Molla, Rani. "Advertisers will spend $40 billion more on internet ads than on TV ads this year," *Recode*. March 26, 2018.

my product, I would be forced to buy advertisements in newspapers, put up billboards in cities, or potentially use direct marketing through the mail (which could cost up to $10 per interaction).[34] While these are effective means of advertising, one result of these methods is that every American would see the same Coca-Cola advertisement regardless of who they were. Regardless of differences in language, gender, or flavor preferences, my Coca-Cola advertisement would be "one-size-fits-all." 100 years later in 2019, a Chief Marketing Officer has entirely new tools at his or her disposal. To advertise Coca-Cola I can create hundreds of variations of the same advertisement to show to hundreds of different skews and segments of customers. The result of this investment is that consumers are more likely to buy a product that they feel is for them. As opposed to the old model of "one-size-fits-all," today's model is focused on "one-size-fits-one." Additionally, rather than spending up to $10 for a mail-order campaign (the cutting-edge advertising technology of 1919), I can use Facebook to pay an average of $1.72 per click on my advertisement in 2019.[35]

These new developments in advertising give social media advertisers the ability to target advertisements to different population segments and discriminate based on various factors of the advertiser's choosing at an extremely cheap price. For instance, a credit agency has the ability to target unique loan advertisements to distinct segments of users – rich, poor, black, or white. Conceivably, these advertisements could present different annual percentage rates (APRs) to each of these different segments of users without any of these individuals ever knowing. In order to maximize sales and profits, advertisers could sell the same product at different prices or in different ways to different buyers through social media. The effect of this would be that individuals would not be afforded equal opportunities because of factors

[34] Bruce, Jenna. "How Much Does Direct Mail Marketing Cots?" *Media Space Solution*. July 31, 2017.
[35] Shewan, Dan. "The Comprehensive Guide to Online Advertising Costs," *WordStream.* January 28, 2019.

that are beyond their control (e.g. race, gender, age). Preventing advertising discrimination is important because it affords everyone the ability to live a good life without being at a disadvantage.

Luckily, however, social media companies are slowly coming around to reducing the ability of advertisers to discriminate through their advertising. For example, in March 2019, Facebook announced that it was "removing age, gender and ZIP Code targeting for housing, employment and credit-related ads" as part of a settlement with advocacy groups and other plaintiffs.[36] This came after the federal government filed a complaint against Facebook for violating the Fair Housing Act, which prevents discrimination in housing.[37] "There is a long history of discrimination in the areas of housing, employment, and credit," wrote Facebook Chief Operating Officer Sheryl Sandberg in a blog post, "and this harmful behavior should not happen through Facebook ads."[38] After realizing that segmented advertisements could hurt some of its users, Facebook reduced discrimination by enforcing standards of electronic informational privacy.[39] Rather than allowing advertisers to access and use all information

[36] Sanberg, Sheryl. "Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising." *Facebook*. March 19, 2019.
[37] Liptak, Andrew. "The US government alleges Facebook enabled housing ad discrimination." *The Verge*. August 19, 2018.
[38] Ibid.
[39] Despite this success, Facebook, and other social media platforms, still have a lot of work to do to prevent discrimination through advertising on their platforms. One prominent example of this can be seen in the world of political advertising and specifically with the case of Cambridge Analytica in the 2016 democratic election of the United States. During the presidential campaign, Cambridge Analytica acquired access to 87 million Facebook profiles. They used the data from these profiles (namely information about what these individuals liked, "friended," and more) to develop psychological profiles about these Facebook users. Subsequently, Donald Trump's team hired Cambridge Analytica to run political advertisements for their campaign and created dozens of variations of political advertisements that encouraged people to vote for Donald Trump. Advertisements that users thought were shown to everyone were specially curated for individuals in a way that other traditional media forms would never have been able to conceive of. This came through Cambridge Analytica accessing identifying facts about individuals from their online profiles and further using these facts to infer traits about individuals. Such an informational privacy violation is unlike other forms of manipulative advertising seen in the past. Now, consider the scenario of Cambridge Analyitica playing out on Billboard instead of on Facebook. If *all* social media information were public, then companies like Cambridge Analytica would be able to even more effectively and easily manipulate users with persuasive advertisements created through psychological profiling. Thus, allowing them to discriminate even further.

about users, Facebook restricted the types of personally personally identifiable information that these advertisers could access and use. By doing this, Facebook utilized electronic informational privacy as a tool for preventing some forms of discrimination through advertising.

In the Billboard State, however, such a solution to the problem of discriminatory would not prevent discrimination on social media because the Billboard State is one that lacks electronic informational privacy. In the Billboard State, all information related to an individual that is present about an individual would be public not only for access, but also for use. Thus, advertisers would be able to build psychological profiles about users based on usage habits in order to finely target advertisements to various groups based on self-serving and possibly discriminatory interests.[40] Landlords would be able to exclude communities of color from seeing housing listings (a 21st century version of the problematic version of red-lining) and employers could request that a job ad not be shown to women or to those over a certain age. In short, any advertiser or individual would be able to use *any* information (e.g. political views, social network, posting habits, or photos) to determine how to present (or not present) information to individuals. The Billboard State opens the door for discrimination against individuals based on anything because the Billboard State does not give social media users electronic informational privacy. Thus, electronic informational privacy is extremely valuable because it protects individuals from discriminatory advertising practices that can infringe on an individual's right to have the opportunity to live their best life.

Social media without electronic informational privacy has the potential to be extremely discriminatory through finely targeted advertisements. However, the value of

[40] Andrews, Edmund. "The Science Behind Cambridge Analytica: Does Psychological Profiling Work?" *Stanford Graduate School of Business*. April 12, 2018.

electronic information privacy is that it protects Internet users from this discrimination and provides individuals with the opportunity to experience life with fewer disadvantages.

Electronic informational privacy is valuable because it is the backbone of values that allow individuals the ability to live a good life. As shown through the Billboard State thought experiment, without electronic informational privacy there would be no way to create intimacy online, facilitate experiments in living, or prevent certain forms of discrimination. When applied specifically to the realm of social media, I find that each of these values relies on electronic informational privacy to truly confer worth to individuals.

IV. PRESERVING PRIVACY, NOTICE-AND-CONSENT ON SOCIAL MEDIA

In appreciating the value of electronic informational privacy, social media platforms operating across the world have accepted their obligation to protect privacy for all users. Generally, these privacy-protecting solutions provide citizens of the Internet with control of their electronic informational privacy by notifying them when their personally personally identifiable information is exchanged or providing social media users the ability to dictate their information exchanges.[41/42]

In this final chapter, I will explore criticisms and responses to notice-and-consent, one of the leading methods used to protect electronic informational privacy. Through analyzing "Terms of Service Contracts," a specific instantiation of notice-and-consent in the world of social media, I hope to describe why terms of service contracts often do not preserve electronic informational privacy even though the idea of notice-and-consent preserves electronic informational privacy. First, I will describe the technical terms "notice-and-consent" and "Terms of Service Contracts" ("ToS"). Then, I will explore two criticisms that ToS do not preserve electronic informational privacy because they do not provide informed consent and may be coercive for signers. Finally I will argue that in spite of these criticisms, there are still ways for social media platforms to protect electronic informational privacy by making ToS easier to understand, changing the format of ToS, and reforming to opt-in nature of ToS contracts.

---

[41] This general principle was first proposed by the Organisation for Economic Cooperation and Development – which has 36 member states including the United States, United Kingdom, Canada, and Germany – in their 1980 report about privacy protection. The OECD report created the standard that, "the processing of personal information requires that its purpose be specified, its use be limited, individuals be notified and allowed to correct inaccuracies, and the holder of the data be accountable to oversight authorities."

[42] OECD. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," *Organisation for Economic Co-operation and Development.* 1980.

What is Notice-and-Consent?

Notice-and-consent is a form of allowing Internet users the ability to control their information by providing notice about a websites data-use practices and subsequently asking users to consent to these practices before engaging with a website. It provides individuals the choice to either engage or disengage with a website based on whether their preferences correspond with the practices of a given website. Notice-and-consent is the current paradigm for consent online and requires communication between online entities and their users.

The paradigm of notice-and-consent holds that in order for informational electronic privacy to be maintained when information is exchanged online, there must be both "notice" and "consent." The "Notice" of notice-and-consent can take various forms of informing users of data-use practices. The General Data Protection Regulation (GDPR) provides a few examples of what this notice may look like:

> *Providing information in writing is the default method, and the guidance refers to various options, including layered privacy statements/ notices, "just-in-time" contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Additional "means" include "videos and smartphone or IoT voice alerts . . . , cartoons, infographics or flowcharts."*[43]

As explained in this legislation, notice can take a variety of forms to communicate to users about what personally personally identifiable information will be accessed and how this personally personally identifiable information with be used.

The "Consent" of notice-and-consent generally arises after a user has been presented with notice. Once they have seen the information as presented, they must be "offered control and a genuine choice in order for consent to be valid" and for electronic informational privacy to be preserved. The action of "consenting" to signify that users accept the terms can

[43] "EU Regulators Provide Guidance on Notice and Consent under GDPR." *The National Law Review*. December 13, 2017.

also take many forms. This action can be active (i.e. clicking an "I agree" button with regards to the notice) or passive (i.e. continuing to use the website after being presented a notice).

Arguments in favor of using notice-and-consent as a method of protecting electronic informational privacy claim that a perfect implementation of this paradigm would ensure that all Internet users can "give free and informed consent to data collection and use practices."[44] This is particularly important because notice-and-consent practices are supposed to guarantee that electronic informational privacy is respected. In such a system, if a user consents to their personally identifiably information being accessed or used in a certain way then their privacy is not violated by the relevant forms of access or use. In this sense, notice-and-consent act as brokers for an acceptable tradeoff between a user's electronic informational privacy and the benefits that websites receive from collecting and using user data.

On social media, notice-and-consent takes the form of ToS.[45] These contracts provide notice by requiring users to either "accept" the ToS before using a platform or refuse the use the platform entirely. These contracts are designed to describe all of the various ways that a user's data can be accessed or used on the platform and, as a result, can often be very long. For example, Instagram's ToS is 17,161 words long – even longer than this senior thesis.[46] The "consent" of ToS is that these users are given as much time as needed to read the ToS contract and subsequently they must agree to the terms. Generally, users only have to indicate their acceptance of ToS once (when they first use a platform) or when there is an

[44] Wagner, Richard and Sloan, Robert. "Beyond Notice and Choice: Privacy, Norms, and Consent." *Chicago-Kent College of Law*. January 2013.
[45] Often times, "notice" on social media is scattered across many different documents (a privacy policy, terms of use agreement, sales agreement, etc.). When I refer to the phrase "Terms of Service Contracts" (ToS), I am referring to the totality of the written rules from social media platforms that address electronic informational privacy. This is because generally a ToS would explicitly refer to these other documents when creating information-use norms. Facebook's ToS is a great example of this as it reroutes interested users to its data policy, advertising policy, platform policy, and more if they are interested in learning more.
[46] Taggart, Emma. "Artist Visualizes the Lengthy 'Terms of Service' Agreements of Popular Social Media Apps." *My Modern Met.* May 23, 2018.

update to the ToS. If a user choses not to consent to the notice, their only option is not to use the platform. Through participating in this process, social media platforms and users can create rules about access to and use of personal personally identifiable information online, thus providing a way to preserve electronic informational privacy when these platforms access or use user information.

On social media platforms ToS is the way that notice-and-consent is provided to users in order to allow them the choice to either engage or disengage with a social media platform and ensure that the access and use of personally personally identifiable information will not violate electronic informational privacy. While ideal when perfectly implemented, this all-or-nothing approach of ToS has quite a few criticisms.

Criticisms of Notice-and-consent

In theory, ToS should maintain electronic informational privacy on social media while promoting the values I described in Chapter 2 (interpersonal intimacy, freedom from discrimination, and an ability to experiment). However, there seem to be two major problems with ToS on social media: the problems of informed consent and binary choice. First, critics argue that ToS contracts do not adequately provide informed consent to social media users who sign them and thus are not contracts that protect electronic informational privacy. Second, these contracts can be viewed as being too manipulative to even constitute a valid contract.

Problem of Informed Consent

The first notable problem with ToS is that people often do not fully understand them which undermines the value of informed consent that ToS are designed to provide to social

media users who sign them. I will define informed consent, describe it's value, and argue that ToS is not an effective means of providing informed consent.

Informed consent is the informed, voluntary, and decisionally-capacitated consent that allows individuals who have read disclosures to engage in a contract. Informed consent requires that individuals agree to engage in a contract after being fully informed of the relevant risks and benefits of a contract.[47] For example, suppose you were about to be admitted to the hospital for a surgery. Before this surgery, doctors would read you all of the benefits of the procedure along with the risks to acquire your consent before operating on you. This process allows patients to engage in informed, voluntary, and decisionally-capacitated consent after notice of all of the facts. In doing so, persons are provided the capacity to determine their destiny rather than having it forced upon them. As Beauchamp & Childress argue in *Biomedical Ethics,* informed consent is important because it recognizes that all persons have unconditional worth.[48]

In the world of social media, informed consent is one of the factors that would allow ToS to be a perfectly implemented notice-and-consent system. Just as a doctor must inform patients of all the benefits and risks of a medical procedure, a social media platform must inform users of all the benefits and risks of sharing personally personally identifiable information. This is because providing informed consent allows full control over personally identifiably information about oneself. If ToS do not provide the information that allows users the capacity to control personally personally identifiable information about themselves, then these ToS would violate electronic informational privacy.

[47] Charland, Louis. "Decision-Making Capacity." *Stanford Encyclopedia of Philosophy*. June 20, 2011.
[48] Beauchamp and Childress. "Principles of Biomedical Ethics." *Oxford University Press.* 2011.

I argue that because many users do not read or understand the ToS that are presented to them, these contracts cannot be seen as being effective methods of acquiring "informed consent" from users. In an interview I conducted with Ryan Graves, the former CEO of Uber, I asked him if he believed that ToS were an effective method of acquiring informed consent from users. His response was simple, "I don't think users will ever spend the time to read a ToS that also meets the requirements of the attorneys."[49] His opinion is similar to many others in the social media and technology industry. This group of privacy advocates argues that almost all Terms of Service contracts and privacy policies are long, unwieldy, and legally jargonistic documents that require repeated, time-intensive reading to understand. Thus, as a result, rather than reading these documents, users simply accept the ToS without being fully informed of what they are consenting to. Skeptical, Jonathan Obar of York University in Toronto and Anne Oeldorf-Hirsch of the University of Connecticut conducted an experiment to investigate if this phenomenon was actually happening.[50] They asked 543 students to register for NameDrop, a new social media platform. In paragraph 2.3.1 of NameDrop's ToS it stated that all these students would agree to give NameDrop their future first-born child. Ultimately, only a quarter of these students read the ToS and all students agreed to use the service.[51] This finding is what led Obar and Oeldorf-Hirsch to call the "I

[49] Graves, Ryan. "Interview with Ryan Graves, former CEO of Uber." Interview by Michael K. Bervell. December 2018.
[50] Obar, Jonathan and Oeldorf-Hirsch, Anne. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society*. April 2, 2016.
[51] More details of the experiment here: All participants were presented the TOS (Terms of Service) and had an average reading time of 51 seconds. Most participants agreed to the policies, 97% to PP (Privacy Policy) and 93% to TOS, with decliners reading PP 30 seconds longer and TOS 90 seconds longer. A regression analysis identifies information overload as a significant negative predictor of reading TOS upon signup, when TOS changes, and when PP changes. Qualitative findings suggest that participants view policies as nuisance, ignoring them to pursue the ends of digital production, without being inhibited by the means. Implications are revealed as 98% missed NameDrop TOS 'gotcha clauses' about data sharing with the NSA and employers, and about providing a first-born child as payment for SNS access.

have read and agree to the terms and conditions" button "the biggest lie on the Internet."[52] I argue that while everyone agreed to give NameDrop their future first-born child, this example is not an instance of informed consent. Informed consent, which is what would allow ToS to be an ideal instantiation of notice-and-consent, relies on the fact that users be informed. However, if users do not even reading the ToS contracts that are supposed to inform them then it is impossible to say that they have given informed consent for social media platforms to access and use their personally personally identifiable information.

Graves' sentiment that users do not read ToS and the finding from the NameDrop experiment is a reflection of the problematic possibility that ToS do not successfully acquire informed consent from users.[53] ToS are designed to create rules about access to and use of personally identifiably information about individuals online; however, if users do not read these contracts then social media platforms are not properly providing users with the informed consent to create new rules related to their electronic informational privacy.

Informed consent is an important component of ToS because it is what allows the exchange of information between users and social media platforms to more closely mimic the principle of notice-and-consent that maintains electronic informational privacy.

[52] Berreby, David. "Click to agree with what? No one reads terms of service, studies confirm." *The Guardian*. March 3, 2017.

[53] Here, we could try to surmise why individuals choose not to read contracts and, consequentially, are not properly informed before asked to consent. As Ryan Graves describes, this may be because ToS are too time-intensive to read. Perhaps, this is because ToS attempt to place every rule about the potential access and use of personally personally identifiable information in one document. However, another reason could be that these contracts are simply too hard to understand even if read. If it is true that people do not read ToS, which seems to be the case, then, regardless of why individuals do not read these ToS, these contracts will not provide users with the ability to make an informed choice about whether or not to agree to new rules related to their electronic informational privacy.

Problem of Binary Choice

The second notable problem of ToS on social media platforms is the lack of negotiating power given to users that are forced to sign them. Most ToS are offered as a binary choice, either users agree to the conditions or they opt to not use the platform at all. I argue that this binary choice undermines the idyllic system of notice-and-consent and results in ToS that do not fully preserve electronic informational privacy because social media users are not given a true opportunity to control their information.

Most ToS are "take it or leave it"; users must either 'consent' or abandon the use of the social media platform. This forcefulness of ToS contracts undermines the ability of users to craft rules about their personally personally identifiable information and instead forces users to unwaveringly accept whatever is placed before them. For instance, I recently purchased a new iPhone and was setting it up for use. After reading Apple's privacy policy, I pressed the "disagree" button. Instead of offering me the opportunity to renegotiate the terms under which I wanted the iTunes Store to use my data, I was bounced back to the page before and forced to try again. Despite my repeated attempts, the only way to exit the endless loop was to accept Apple's terms. Instead of freely being able to dictate the rules with which I wanted to control my personally personally identifiable information, I was forced to accept Apple's terms or not use an iPhone at all.

One could similarly argue that users of social media platforms actually do not have the ability to dictate the rules governing their information and are instead are forced to accept an unscrupulous set of electronic informational privacy rules set out by social media platforms. Mark Lemley aptly highlights this problem in his 2006 Minnesota Legal Review paper, *Terms of Us*e: "Assent by both parties to the terms of a contract has long been the

fundamental principle animating contract law. Indeed, it is the concept of assent that gives contracts legitimacy and distinguishes them from private legislation."[54] From here, Helen Nissenbaum so aptly links this requirement of contracts to ToS by arguing that "while it may seem that individuals freely choose to pay the informational price, the price of not engaging socially, commercially, and financially may in fact be exacting enough to call into question how freely these choices are made."[55] ToS are problematic because signers of these contracts only have weak instantiations of choice and autonomy to manipulate contracts. Lemley argues that when presented with a ToS, social media users must voluntarily and without coercion enter into the contract if we are to say that the ToS protects electronic informational privacy. Since a forced contract does not represent the will of the signer, it cannot entail moral obligation. Moreover, ToS as they exist do not give social media users the ability to write the rules that will govern their identifying information if they choose to use a platform.

This issue is problematic because it undermines the necessary condition of contracts that contract signers are free from coercion when they make the decision to enter into a contract. Since social media platform ToS force users to either consent or leave without the opportunity for discussion, individuals are not freely entering into a contract of their choosing. For ToS to be used as rule-defining contracts that apply to electronic informational privacy, they must be valid contracts that are entered by the signers at the signer's will. This matters because a ToS that coerces users to provide consent undermines users' control over their personally personally identifiable information. A fair ToS contract would offer options such as partial acceptance or the ability to craft a responsive contract that promotes the signers' autonomy and freedom to control their electronic informational privacy.

---

[54] Lemley, Mark. "Terms of Use." *Minnesota Legal Review.* 459, 464–65. 2006.
[55] Nissenbaum, Helen. "A Contextual Approach to Privacy Online." *Daedalus.* Fall 2011.

Perhaps the most emphatic response to this problem is that users have no obligation to use social media platforms. Thus, even though the problem of binary choice exists it is not problematic because users can simply opt to not use a platform rather than subjecting themselves to ToS that do not preserve electronic informational privacy. While this is true, electronic informational privacy is focused on maximizing user control over their personally personally identifiable information online. Thus, the control-maximizing solution for users would be to allow them the ability to use platforms in ways that mirrored limited information-use rather than requiring that users abandon every social media platform with binary ToS.

While social media platforms may be trying to institute a perfect version of notice-and-consent to protect electronic informational privacy through ToS, it seems that these contracts, though perfect in theory, might actually undermine the values of electronic informational privacy in practice because of the problems of binary choice and informed consent.

Privacy-Preserving Modifications to Notice-and-consent

Despite the problems with ToS as they exist, it seems plausible to imagine a revised versions of these contracts that are a more ideal instantiation of notice-and-consent while also protecting electronic informational privacy for all social media users. With changes, the ToS system could preserve informational privacy and its values of preserving intimacy, promoting autonomy, and permitting experiments in living. I argue that digestible ToS, prompted ToS, and opt-in ToS can address the problems of length-induced convolution and poor negotiating powers of ToS on social media platforms. At the end of this section, I will run through a case study to describe how these changes would look for users.

Digestible Terms of Service Contracts

The first major criticism of ToS was that they did not properly provide informed consent to users of social media platforms. In an attempt to remedy this criticism of ToS, I suggest some version of digestible or summarize ToS. These summaries could tease out the parts of contracts that affect the electronic informational privacy of users in layman's terms. By doing this, ToS would actually give users the opportunity to provide informed consent by giving users the ability to actually read these complex contracts. Subsequently, users would be able to have more control over their information by having an idea of what they are actually consenting to.

This digestible ToS could take multiple forms. One example is what Ryan Graves suggested, "a standard set of basic ToS principles between all services." Graves describes some sort of common-principle that is shared amongst all social media platforms that would allow users to synthesize the complexities of ToS contracts by making them more recognizable. Such a proposal would rely on shared electronic informational privacy norms generated by social media platforms or the law that reflect the expected hopes of users. Another example of digestible ToS are "too long; didn't read" summary clauses at the beginning of a ToS in addition to links to particular parts of the ToS.[56] This solution is one I heard described by Dennis Crowley, the founder of Dodgeball and Foursquare, "I imagine that many sites will start to adopt at TL;DR version of the Privacy and TOS documents."[57] In fact, it was a solution that Crowley's team was looking to implement for Foursquare which

[56] Gil, Paul. "What is 'TLDR'?" *Lifewire.* January 25, 2019.
[57] Crowley, Dennis. "Interview with Dennis Crowley, founder of Foursquare." Interview by Michael K. Bervell. December 2018.

has over 50 million users.[58] Ideally, these versions of ToS will give individuals the ability to control their electronic informational privacy by actually making them understandable at a glance *and* upon deeper inspection.

Prompted Terms of Service Contracts

Another solution to make ToS a more ideal instantiation of notice-and-consent would be prompted ToS. This solution would repeatedly prompt users with notice and require their consent as they use social media platforms rather than the current model of one-time notice at the onset of using a platform or when the platform's ToS is updated. These prompts could be displayed at times when users would most willing to read ToS notices or when users are about to engage in an action that could potential violate their electronic informational privacy, thus ensuring that when users consent they are actually providing informed consent. This would bring ToS one step closer to the perfect implementation of notice-and-consent.

The value of prompted ToS also stretches beyond simply informed consent: these prompts allow users to escape the problem of binary choice, the issue of ToS contracts that require users to either accept every condition or stop using the platform. By providing users notice and require consent only when absolutely needed, platform will better protect users' electronic informational privacy by providing users more control. Rather than requiring consent for *all* information from users, the prompted ToS allows platforms to request consent for *some* information. By utilizing prompted ToS, platforms both limit the amount of personally personally identifiable information they receive while also offering more opportunities for control to users.

[58] Weber, Harrison. "Foursquare by the numbers: 60M registered users, 50M MAUs, and 75M tips to date." *Venture Beat.* August 18, 2015.

Opt-in Terms of Service Contracts

A final solution for addressing the problems of ToS is having opt-in, rather than opt-out, contracts. I argue that by shifting the frame of ToS from "opt-out" to "opt-in," social media users will have the opportunity to negotiate what personally identifiable information is shared with platforms, thus providing them more control. This specifically addresses the second criticism of ToS, that they do not allow signers the ability to negotiate their contract and consequentially coerce users to sign contracts that undermine their ability to control their electronic informational privacy.

Generally, opt-in is the process used to describe when a positive action is required in order to consent while opt-out implies that a user is more easily signed up for a service and must actively take an action to remove consent. This distinction could be as simple as requiring that users actively have to select check boxes to create rules about access and use of their information before consenting to a ToS rather than after consenting to a ToS. In this sense, users would have direct and immediate control of the contract that governs how their identifying information is used. If these changes were made, then users would have control over how their electronic informational privacy is both accessed and used. This is the approach that the data protection agency of the UK describes as "the safest way of demonstrating consent."[59]

The paradigm of notice-and-consent is designed to provide Interner users with a way to protect their electronic informational privacy by being notified when their personally personally identifiable information is being accessed or used and consenting to this access or use. However, in the world of social media the instantiation of notice-and-consent through ToS is not an effective way of protecting the electronic informational privacy of social media

[59] "Direct Marketing." *Information Commissioner's Office.*

users because of the problems of informed consent and binary choice. Nevertheless, ToS are not a lost cause because it is possible to make revise these contracts to give users more control of there electronic informational privacy by crafting digestible, prompted, and opt-in ToS.

V. CONCLUSION

With the rise of social media technology came a reform in how individuals engage with one another. Instead of gathering at a town square to exchange news, citizens turn to the digital town square of social media platforms. Similarly, social media users now look to have intimate spaces similar to a digital living room to connect with one another on the platforms they use every day. As Mark Zuckerberg aptly described in a March 6, 2019 Facebook post on privacy:

> *Over the last 15 years, Facebook and Instagram have helped people connect with friends, communities, and interests in the digital equivalent of a town square. But people increasingly also want to connect privately in the digital equivalent of the living room. As I think about the future of the internet, I believe a privacy-focused communications platform will become even more important than today's open platforms. Privacy gives people the freedom to be themselves and connect more naturally, which is why we build social networks.*[60]

Both online and offline, people have an expectation of privacy when communicating with one another.

Electronic informational privacy as I defined it is the following of rules about access to and use of personally identifiable information about oneself online. If online entities follow these rules (which can be created through social norms or voluntary agreements) when both accessing and using personally identifiable information then the expectations of privacy people have will be respected.

Respecting electronic informational privacy in the world of social media allows individuals to experience three values that allow them to live a good life. First, respecting this electronic informational privacy preserves the ability of people to make intimate relationships online, a phenomenon that makes life more fulfilling. Second, electronic

[60] Zuckerberg, Mark. "A Privacy-Focused Vision for Social Networking." *Facebook*. March 6, 2019.

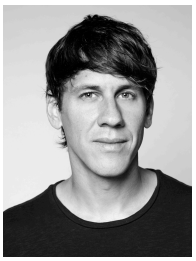
informational privacy permits Millian experiments in living that allow individuals to develop without the patronizing gaze of the public. Third, electronic informational privacy protects social media users from forms of discrimination that would otherwise limit the ability of people to decide their own fate in life.

As companies face new concerns over electronic informational privacy concerns on their platforms, they must take a hard look at revising their current methods of protecting this privacy for users. On social media, this specifically includes examining notice-and-consent, a principle that requires platforms to provide notice to users and obtaining their consent before collecting or using their personally identifiable information. Today, terms of service Contracts are an instantiation of the principle of notice-and-consent; however, they are not perfect and, as such, could be improved to better protect electronic informational privacy. In their current form these contracts reduce the amount of control that social media users have over their data because they lack in their ability to properly garner informed consent from users and only offer users a limited number (i.e. binary) of control options. While solving these problems may not happen with one change, some slight changes can serve to make terms of service contracts better at implementing notice-and-consent and protecting electronic informational privacy. First, these contracts could be easier to understand by being shorter; second, these contracts could require repeated consent rather one-time consent; and third, these contracts could focus on better garnering opt-in consent rather than opt-out consent.

Philosophers, social media companies, and the public all have a stake in ensuring that informational privacy is not lost online or on social media platforms. As life becomes digital and people strive to connect through the internet, the problems of electronic informational

privacy will only continue to grow. The good life does not need to be one that is separate from the online life; however, the good life on social media is one that must constantly be under critical, philosophical evaluation.

Appendix A: Interview with Dennis Crowley, Foursquare founder
Interview conducted by Michael Bervell in December 2018.


Dennis Crowley

Dennis Crowley (born June 19, 1976) is an American Internet entrepreneur who co-founded the social networking sites Dodgeball and Foursquare.

<My question> How do you define "data privacy"? Should this definition be different for celebrities ("very important people") versus non-celebrities ("regular people")?

If celebs want to put certain things out in public (e.g. public Twitter account, public IG account, etc) that's one thing, but as a default, all "users" of these services should be treated the same. They should own their data, have the right to see it / delete it whenever they want, and have a right to know if and how it's being used both on and off the service.

<My question> Theorists argue that we live in a new era of "surveillance capitalism," where individuals use products for free and companies make profits from their data. Who should be held responsible for ensuring privacy in such a system?

The "users" trust the "services" with save-guarding their privacy, and it's the "services'" responsibility to honor the trust the users put in them.

<My question> All users of digital platforms must agree to "terms of service" (ToS) clauses. Based on your experience, do you think user interactions with ToS be updated in some way? I ask this question with a particular eye towards the rise of data sharing to third-parties by platforms.

I do think most TOS are very very very dense -- too dense for the average user to read / comprehend. I imagine that many sites will start to adopt at TL;DR version of the Privacy and TOS documents. <off record>We've had this discussion internally — the TL:DR version is something we're committed to doing. but we haven't finalized language yet</off record>

Hope that's helpful!
Ping me w/ any follow ups! –d

Appendix B: Interview with Ryan Graves, former CEO of Uber

Interview conducted by Michael Bervell in December 2018.

Ryan Graves

Ryan Graves is an American businessman. He is the Founder & CEO of Saltwater. Graves was formerly the CEO, then SVP of Global Operations at Uber, where he remains on the board of directors.

<My question> How do you define "data privacy"? Should this definition be different for celebrities ("very important people") versus non-celebrities ("regular people")?

data privacy in my view should be data control, you a) know what data exists, b) know who is accessing it, c) have control over it (can retract access or even delete it if the user wishes) if we can apply those concepts, it should be the same for everyone.

<My question> Theorists argue that we live in a new era of "surveillance capitalism," where individuals use products for free and companies make profits from their data. Who should be held responsible for ensuring privacy in such a system?

we likely need regulation to do this, I'm all for capitalism but I don't think corporations have a great history of making the right decisions in these types of cases. features should be limited if the user chooses to share limited information... it's a transaction.

<My question> All users of digital platforms must agree to "terms of service" (ToS) clauses. Based on your experience, do you think user interactions with ToS be updated in some way? I ask this question with a particular eye towards the rise of data sharing to third-parties by platforms.

i don't think users will ever spend the time to read a ToS that also meets the requirements of the attorneys. given this is the case a standard set of basic ToS principles between all services could be helpful, but we're a long way from that.

REFERENCES

88th United States Congress. "Civil Rights Act of 1964." July 2, 1964.

116th United States Congress. "Mark Zuckerberg Hearing Before The United States Senate Committee On The Judiciary And The United States Senate Committee On Commerce, Science And Transportation." *United States Senate.* April 10, 2018.

Andrews, Edmund. "The Science Behind Cambridge Analytica: Does Psychological Profiling Work?" *Stanford Graduate School of Business*. April 12, 2018.

Beauchamp and Childress. "Principles of Biomedical Ethics." *Oxford University Press.* 2011.

Berreby, David. "Click to agree with what? No one reads terms of service, studies confirm." *The Guardian*. March 3, 2017.

Bevanger, Lars. "Norway: The country where no salaries are secret," *BBC.* July 22, 2017.

Blaauw, Pieters, Van den Hoven, and Warnier. "Privacy and Information Technology." *Stanford Encyclopedia of Philosophy*. November 20, 2014.

Bruce, Jenna. "How Much Does Direct Mail Marketing Cots?" *Media Space Solution*. July 31, 2017.

Campbell, Steve. "How do Social Networks Make Money?" *Make Use Of.* April 30, 2010.

Charland, Louis. "Decision-Making Capacity." *Stanford Encyclopedia of Philosophy*. June 20, 2011.

Crowley, Dennis. "Interview with Dennis Crowley, founder of Foursquare." Interview by Michael K. Bervell. December 2018.

"Direct Marketing." *Information Commissioner's Office.*

"EU Regulators Provide Guidance on Notice and Consent under GDPR." *The National Law Review*. December 13, 2017.

"Finstagram – a secret Instagram account to post ugly selfie," *The Guardian*. February 21, 2017.

Fried, Charles. "Privacy," *Yale Law Journal*. 1968.

Gil, Paul. "What is 'TLDR'?" *Lifewire.* January 25, 2019.

Graves, Ryan. "Interview with Ryan Graves, former CEO of Uber." Interview by Michael K. Bervell. December 2018.

Harper, Gary. "The Internet's Multiple Roles in Facilitating the Sexual Orientation Identity Development of Gay and Bisexual Male Adolescents." *American Journal of Men's Health.* January 13, 2015.

Horrigan, John. "Online Communities." *Pew Research Center.* October 31, 2001.

"How Many Bald People Live on Earth?" *Quora*. December 14, 2017.

Kerby, Justin. "Here's How Much Facebook, Snapchat, and Other Major Social Networks are Worth." *Social Media Today*. May 16, 2017.

Liptak, Andrew. "The US government alleges Facebook enabled housing ad discrimination." *The Verge*. August 19, 2018.

Lucero, Leanna. "Safe spaces in online places: social media and LGBTQ youth." *Multicultural Education Review.* April 12, 2017.

Mill, John Stuart. "On Liberty." *Longmans, Green, Reader and Dyer*. 1859.

Molla, Rani. "Advertisers will spend $40 billion more on internet ads than on TV ads this year," *Recode*. March 26, 2018.

OECD. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," *Organisation for Economic Co-operation and Development.* 1980.

Rachels, James. "Why Privacy Is Important." *Princeton University Press*. 1975.

Read, Ash. “The News Feed is Outdated: How Stories Changed the Way I Think About Social Media.” *Buffer*. November 16, 2018.

Lemley, Mark. “Terms of Use.” *Minnesota Legal Review.* 459, 464–65. 2006.

Nissenbaum, Helen. “A Contextual Approach to Privacy Online.” *Daedalus.* Fall 2011.

Nissenbaum, Helen. “Privacy in Context: Technology, Policy, and the Integrity of Social Life.” *Stanford University Press*. November 24, 2009.

“Number of social media users worldwide from 2010 to 2021 (in billions).” *Statista.* July, 2017.

Obar, Jonathan and Oeldorf-Hirsch, Anne. “The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services.” *Information, Communication & Society*. April 2, 2016.

Parent, William. “Privacy, Morality, and the Law,” *Philosophy & Public Affairs.* Page 270. Autumn 1983.

“Percentage of U.S. population with a social media profile from 2008 to 2019” Statista. March, 2019.

Sanberg, Sheryl. “Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising.” *Facebook*. March 19, 2019.

Shewan, Dan. “The Comprehensive Guide to Online Advertising Costs,” *WordStream.* January 28, 2019.

Taggart, Emma. “Artist Visualizes the Lengthy ‘Terms of Service’ Agreements of Popular Social Media Apps.” *My Modern Met.* May 23, 2018.

United States. Securities and Exchange Commission. *Facebook: Form 10-Q.* 31 December 2017.

United States. Securities and Exchange Commission. *Twitter: Form 10-Q.* 31 December 2017.

Vaillant, George. "Triumphs of Experience: The Men of the Harvard Grant Study." *Belknap Press*. 2012.

Wagner, Richard and Sloan, Robert. "Beyond Notice and Choice: Privacy, Norms, and Consent." *Chicago-Kent College of Law*. January 2013.

Weber, Harrison. "Foursquare by the numbers: 60M registered users, 50M MAUs, and 75M tips to date." *Venture Beat.* August 18, 2015.

Wichter, Zach. "2 Days, 10 Hours, 600 Questions: What Happened When Mark Zuckerberg Went to Washington." *The New York Times.* April 12, 2018.

Zuckerberg, Mark. "A Privacy-Focused Vision for Social Networking." *Facebook*. March 6, 2019.