“We are at a pivot point in US privacy history”: An Interpretive Policy Analysis of the Existing US Federal Privacy Regulatory Framework for Lifestyle & Wellness Wearable Technologies

Elisabeth Bassini

Primary Mentor: Emily Mendenhall

A Thesis Submitted in Partial Fulfillment of the Requirements for the Award of Honors in Science, Technology, and International Affairs, Edmund A. Walsh School of Foreign Service, Georgetown University, Spring 2019
ACKNOWLEDGMENTS

Professor Mendenhall - Thank you for your continuous support for both my work on my thesis and my passion for tech policy. I greatly appreciate the advice that you provided me regarding how to select a methodology. Your assistance was invaluable!

Professor Prescott – Thank you for providing me with advice regarding how to narrow the scope of my thesis topic.

Professor Jones – Thank you for offering to speak with me on numerous occasions regarding the legal aspect of my thesis and connecting me with your contacts in the US privacy community.

Family and Friends – Thank you so much for reading my drafts and being incredibly supportive!

DISCLAIMER

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the US Government. Nothing in the contents should be construed as asserting or implying US Government authentication of information or endorsement of the author’s views.
ACRONYMS

-US – United States of America
-EU – European Union
-FTC – Federal Trade Commission
ABSTRACT

In part as a result of numerous devastating data breaches, along with the 2018 passing of comprehensive privacy legislation by both the EU and the US State of California, the US Congress began to discuss whether the federal government should modify its approach to privacy moving forward. With a focus on lifestyle and wellness wearable technologies (hereafter, “wearables”), due to their growing use in the EU and the US, the thesis uses the qualitative, interpretive policy analysis methodology introduced by Dvora Yanow (2000) to capture the discourse within and between three policy-relevant interpretive communities in the US privacy community. In particular, the thesis provides valuable insight regarding: their framing of data privacy for wearables; their evaluation of the existing US federal government’s privacy legislation for wearables; and their perception of how the federal government should approach ensuring consumer privacy for these technologies moving forward. In addition, for comparison purposes, the thesis analyzes interview transcripts from an interpretive community, consisting of European Commission-level officials, regarding its framing of privacy and its evaluation of the Commission’s privacy framework for wearables. The thesis argues that there is a widespread consensus among the communities that the US federal government’s existing privacy regulatory framework for wearables is inadequate and that change is needed. Nevertheless, determining how the US federal government should proceed with approaching privacy will be very difficult as these communities have divergent interests that impact their perception of what this approach should look like moving forward. The thesis highlights the interest of the US communities in strengthening the FTC’s enforcement capability and creating research programs that incentivize companies to design technologies that protect the privacy of wearables users, while not restricting the ability of the wearable to operate. Moreover, while the divide over how to proceed in the US is evident, the analysis of the European Commission community’s perspective on privacy and its legal framework for privacy highlights that the US communities share more consensus regarding privacy than they do with other global models. Therefore, although determining how the US federal government should move forward with approaching privacy will be very difficult, these findings suggest that a focus on prioritizing the shared US values of innovation and privacy may be the best option for federal policymakers. Moreover, the thesis reveals that further research should be pursued to fill gaps that still exist in our understanding of which US federal privacy approach would be most beneficial for smaller technology companies or startups.
SECTION 1: INTRODUCTION

In recent years, concern for privacy has grown within the US in part as a result of findings that certain companies have been using data collected on users to reveal sensitive information and to exploit user data through third party sales (Madden & Rainie, 2015). In January 2018, Strava, a fitness tracking company, was found to be inadvertently releasing sensitive information about its users online in the form of a heat map on its website. The map displayed the location and staffing of US military bases and outposts and the running routes of most of its users, which made many individuals begin to question the privacy guarantees for the data collected by their lifestyle and wellness wearable technologies (hereafter, “wearables”). Moreover, in January 2018, the finding that Cambridge Analytica, a political firm, was able to acquire access to private data on millions of Facebook users sparked concerns about how user information on social media platforms is protected.

The reaction of many Americans to the discovery of how their data is being used suggests that many Americans value their privacy and having their data protected from exploitation (Kunchakarra et al, 2017). Yet, these concerns have faced increasing tension with certain services offered by new technologies that are unable to operate without collecting and sharing user data. This phenomenon of the privacy concerns of consumers not aligning with their privacy habits and decisions is called the “privacy paradox” (Motiwalla & Li, 2016). Recent surveys by the Pew Research Center highlight this privacy paradox (Madden & Rainie, 2015). The Center found that only 9% of over 607 Americans surveyed believe that they have “a lot of control” over the information that is collected about them, and 74% responded that having control over who can access this data is very important to them (Ibid.). Yet, as of March 2018, about 69% of American
adults still used some kind of social media platform, like Facebook, even though these services collect data on them (Ibid.).

This paradox between how highly many Americans value privacy and their continued use of these data-collecting technologies suggests that many Americans have come to depend on these technologies for their convenience and growing importance to modern life activities. Moreover, despite these infringements on their privacy, users will most likely continue to use these technologies and expect these privacy intrusions. This is particularly true for wearables, which are the focus of this thesis, because, despite knowing the risks, many people continuously engage in daily use of these technologies. Thus, in an age of information technology, government regulators, privacy advocates, companies, academicians, and citizens struggle to navigate what new technologies mean for privacy and what role the government should play in regulating these technologies and ensuring consumer data privacy.

With the rise of new technologies like Internet of Things (IOT) devices, the increasing accuracy and bulk of user data collected by these devices have raised the importance in the West of assessing the implications of these technologies for privacy (Federal Trade Commission, 2015; OECD, 2016). For example, wearables, like the sleep-monitoring FitBit Ionic, collect data on users, such as the time, duration, and proximity of an activity, that allow users to track their everyday health metrics to improve their lifestyle habits. Yet, when these data are combined with other types of data, like demographic data, there is concern that this information results in harm for the user by providing valuable information about their physical health and emotional wellbeing. This data could be exploited for third-party sales or be used for inappropriate monitoring, informal screening, target marketing, and potential discriminatory actions (Kunchakarra et al., 2017).
Moreover, incidents, like Strava and Cambridge Analytica, have garnered immense attention in the US regarding privacy and have raised the question of how privacy can and should be safeguarded in an age of big data technologies. While a single data point collected from these IOT devices may not seem valuable, the ability of advertisers or individuals with mal-intent to aggregate these data points to determine trends about individuals should not be underestimated. Wearables exemplify this risk: in 2012, the Federal Trade Commission (FTC) revealed that twelve health and fitness apps, that use data from wearable devices, sold user data to seventy-six different third parties, which raised concern within the US regarding transparency about the actual privacy of user data from third party use (Kunchakarra et al., 2017).

In part as a result of this growing demand by users globally for greater privacy protection, in 2018, the US federal government observed a flurry of privacy legislation being implemented by foreign governments, like the European Union (EU), and US states, which has sparked discussion in Congress about whether the US federal government should modify its approach to privacy moving forward. In May 2018, the EU put into force its overarching privacy framework for the processing of data called the General Data Protection Regulation (GDPR). Some Western media and privacy experts have begun to claim that the European Commission’s approach to protecting the privacy of user data is much more comprehensive and beneficial for the individual than the US federal government’s existing sectoral privacy framework (The Economist, 2018; Sepulveda, 2018). This debate only became more heated when in October 2018, the US State of California passed the ‘California Consumer Privacy Act 2018’ (CCPA) that places even greater protections on consumer privacy and includes similar privacy concepts to those presented in the GDPR (Sepulveda, 2018). These similar privacy concepts include: allowing users to opt out of certain
types of data processing and to be forgotten through requesting that their data be deleted from a database (Sepulveda, 2018).

CCPA has resulted in a flurry of discussion within the US privacy community surrounding whether a federal or ‘national’ privacy legislation should be put in place. So far, different stakeholders or “interpretive communities” in the US privacy community have differed in their perception of what a ‘good’ US federal government approach to protecting data privacy would look like, possibly as a result of different interpretations of the value and meaning of ‘privacy’ (Benioff, 2018; Kang, 2018; Roose & Kang, 2018). For example, most of the private sector sees the creation of a national privacy legislation as beneficial because companies can more easily comply to one set of national legislation rather than the patchwork of privacy legislation that currently exists in the US at the federal and state levels (Benioff, 2018; Kang, 2018; Roose & Kang, 2018; U.S. Chamber of Commerce, 2018). Conversely, privacy advocates see the implementation of a national privacy legislation as a negative move since the legislation would preempt all state-level privacy legislation and may provide less protections for consumer privacy than exist in some states currently (Kang, 2018; Roose & Kang, 2018). These two perspectives of different interpretive communities in the US suggest the various interpretations of the meaning of ‘privacy’ and the different perceptions of how the US federal government should approach privacy moving forward.

The existing literature fails to address the discourse within and between various interpretive communities that serve as stakeholders in the US privacy community. This may be in part attributed to the fact that these communities exist amidst a shifting time in US privacy, with the introduction of the GDPR, the disruption of the Cambridge Analytica and Strava incidents, the passing of CCPA, and the occurrence of numerous US company data breaches. Moreover,
wearables are currently undergoing rapid transformation in real time – underscoring the complexity and speed through which people are learning to use, adapt, and protect their privacy while using these tools. Scholars up to this point have primarily focused on arguing about the history of how people have labeled and framed privacy in the West; the privacy implications of a growing use of more advanced, data collecting technologies; evaluating through legal analysis the existing US federal government’s privacy framework with a growing use of these more advanced, data collecting technologies; and assessing how the US federal government should approach privacy for wearables moving forward based on these legal analyses.

This thesis seeks to analyze the different perspectives of interpretive communities in the US privacy community associated with wearables. It asks: How is privacy labeled and framed by policy-relevant interpretive communities in the US? How does this framing relate to their evaluation of the existing US federal government’s regulatory framework for protecting data privacy for wearables? Finally, how does this framing relate to their perception of how the US federal government should approach privacy for these technologies moving forward? The thesis argues that there is widespread consensus among policy-relevant interpretive communities that the US federal government’s existing privacy regulatory framework for wearables is inadequate and that change is needed. Nevertheless, determining how the US federal government should move forward with approaching privacy will be very difficult because these communities have divergent interests that impact their perception of what this approach should look like moving forward.

This thesis captures the different evaluations and perceptions of these interpretive communities at a time of uncertainty in the US about the ‘effectiveness’ of the US federal government’s existing privacy regulatory framework. This project appeals to the policymaking
community that will be able to use the analysis of these communities to inform future decision-making regarding the US federal government’s approach to privacy for wearables.

**METHODS AND CONTEXT**

This thesis uses the qualitative, interpretive policy analysis methodology introduced by Dvora Yanow (2000) to provide valuable insight into the evaluations of policy-relevant interpretive communities in the US privacy community. It focuses on interpretive community members’ views of the US federal government’s existing regulatory framework for protecting data privacy for wearables and their perception of how the US federal government should approach privacy for these technologies moving forward (Yanow 2007, pp. 10). Interpretive policy analysis is used for this thesis to understand how different US interpretive communities: frame the policy-issue of privacy for wearables; evaluate what the existing US federal government’s privacy regulatory framework for wearables means to them; and, based on their privacy framings, perceive how the federal government should approach ensuring consumer privacy for these technologies moving forward. The documents analyzed to determine the community discourse include transcripts from semi-structured interviews, primary policy documents, organization reports, organization websites, and newspaper articles.

This thesis focuses on three policy-relevant interpretive communities, including 33 individuals, who participated in in-depth qualitative interviews between May 2018 and November 2018. These interviews aimed to capture discourse between the communities and contribute to existing knowledge through providing different interpretations of the current federal privacy regulatory framework for wearables. These interpretive communities include: the US federal government, the private sector, and public interest groups. In my analysis, the public interest groups community is divided into two sub-groups: pro-industry and pro-consumer protection.
Interview subjects were placed in the pro-industry public interest group community if their organization stated on their website that the organization is: funded by industry, advocates for industry interests, or the subject mentioned in the interview that the majority of the organization’s funding comes from industry. This analysis provides a snapshot of the inter- and intra-community discourse at this time of uncertainty in US history through analyzing how interpretive communities differently evaluate the current federal privacy framework, and how they perceive that the US federal government should approach privacy for these technologies moving forward. In addition, for comparison purposes, the thesis analyzes interview transcripts from an interpretive community, consisting of European Commission-level officials, regarding its framing of privacy and its evaluation of the Commission’s privacy framework for wearables.

In what follows, this thesis provides a brief background of the history of how people have labeled and framed privacy in the West. It presents previous evaluations of the current federal privacy framework for wearables, and addresses existing perceptions of how the US federal government should approach privacy for new technologies. Then, the thesis discusses the interpretive policy analysis methodology and outlines how the interpretive communities label and frame privacy, evaluate the current federal privacy framework for wearables, and perceive how the US federal government should approach privacy for wearables moving forward.
SECTION 2: LITERATURE REVIEW

2.1. EVOLUTION OF PRIVACY DEFINITION IN THE WEST

Historical perceptions of privacy have evolved over time in the West by region and time period. These changes have largely responded to the emergence of new technologies and necessarily continuous reevaluations of how privacy is perceived. In the West, privacy first began being discussed in philosophy circles in Ancient Greece by philosophers such as Aristotle (Hongladarom, 2016). Aristotle argued that privacy referred to the distinction between the public sphere of political activity and the private sphere associated with family and domestic life (Ibid). In Roman times, the definition of privacy evolved to become associated with the protection of an individual’s “private property” from others or the concept that one’s private domain was her own house (DeCew, 2018). For example, individuals of this time demanded that in their houses their conversations should be private and not intruded upon by surveillance, like the presence of soldiers (Ibid).

During the Enlightenment, the definition of privacy expanded to include that, in addition to private property, the state or condition of one’s thoughts or ideas should also not be observed or disturbed by other people (Hongladarom, 2016). This definition of privacy, therefore, extended beyond the concept of private property, to include that one’s private thoughts and ideas should also not be disturbed by other people (Ibid). This expanded concept of privacy to include one’s thoughts, ideas, and subjectivities was as a result of the belief of modern philosophers that these thoughts were the underpinning of epistemology and metaphysics (Ibid). For example, in his works, philosopher René Descartes (1968) supports this expanded definition of privacy by arguing that all knowledge is founded on one’s sense of subjectivity of himself as a thinking, conscious being, suggesting the value of one’s consciousness and the importance that this consciousness is
private. Yet, it was impossible to predict how technologies would develop. These early philosophers could not possibly have predicted the implications of new technologies that can surveil individuals in their homes and potentially use the data collected to identify trends in a user’s thought patterns. Thus, these earlier definitions of privacy were naturally challenged by scholars who argued that these definitions oversimplified the concept of privacy and failed to take into account the complexity of more advanced, data collecting technologies.

In recent years, some scholars have argued that previous definitions of privacy do not adequately address the existence of more advanced, data collecting technologies in today’s society, and have called for a reevaluation of how the term ‘privacy’ is defined (Parent, 1970; Solove, 2004). William Parent (1983), for example, frames privacy more generally as others possessing one’s private information and emphasizes the importance of ensuring the informed consent of the user to how their data are used and shared. Parent (1983) argues that “Privacy is the condition of not having undocumented personal knowledge about one possessed by others...[and that] a person’s privacy is diminished exactly to the degree that others possess this kind of knowledge about him” (269). In contrast, legal scholar Robert Post (2001) argues that previous definitions of privacy, like those of Parent, oversimplify privacy. Post (2001) instead emphasizes the potential fruitfulness of attempting to decipher the “competing and contradictory dimensions, so engorged with various and distinct meanings, that [he] sometimes despair[s] whether it can be usefully addressed at all” (2087). Scholars like Daniel Solove (2004) support Post’s sentiment that the definition of privacy has become too oversimplified, arguing that “privacy” must be understood as “a general term that refers to the practices we want to protect and to the protections against disruptions to these practices” (1093) and that “we should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted” (1093). Further, Solove (2004)
perceives privacy as having a different definition depending on the situation, and as a result, advocates for the creation of charts and taxonomies to provide more specific definitions of privacy through assessing the privacy violations posed by different technologies.

2.2. PRIVACY IMPLICATIONS OF NEW TECHNOLOGIES

Important metaphors and values have arisen to assess the privacy implications of individual new technologies and the importance of data privacy protection. Many scholars have argued for the importance of privacy with the rise of new technologies through focusing on the harms posed by these technologies (Parent, 1983; Solove, 2004). Yet, these arguments often overgeneralize the risk of new technologies for privacy since all technologies pose different risks. These arguments also often fail to consider other value judgements when individuals are deciding whether privacy is important. For example, some individuals believe that privacy should always be ensured for health data collected by new wearables, but some individuals believe that the privacy of this data is less important than the convenience of having their steps tracked on their phones for easier health monitoring (Rainie & Duggan, 2016).

Two major scenarios have emerged in the literature that focus on assessing the privacy implications posed by different technologies and arguing for the importance of ensuring data privacy with the rise of these technologies based on these implications. Solove (2004) coined these two scenarios as 1. ‘The Big Brother’ government surveillance metaphor or “scenario” (29) and 2. ‘The Trial’ exploitation-of-user-individuality scenario, to capture common arguments in the literature surrounding the privacy implications of new technologies (36).

‘The Big Brother’ scenario focuses on the privacy implications of database technologies like computers (Solove, 2004). This metaphor suggests that these technologies enable the government to use them for increased surveillance purposes, and therefore, frames privacy as very
important in ensuring that the thoughts and property of these individuals are not bothered when database technologies are used (Ibid). ‘Big Brother’ refers to George Orwell’s (1949) depiction in his book *1984* of an all-knowing, constantly vigilant government that regulates every aspect of one’s existence using technology. In this surveillance state, sociologist Dennis Wrong (1979) argues that “men [and women] are deprived of the very capacity for cherishing private thoughts and feelings” (115). This ideology was perpetuated in 1974, when US Supreme Court Justice William Douglas referred to the implications of technology for enabling this surveillance when he stated that the computer, in particular, has become “the heart of a surveillance system that will turn society into a transparent world” (Sampson vs Murray 1974, pp. 415). This scenario suggested that the databases created by these data-collecting technologies will ensure that no secrets can be held. Legal scholar Jerry Kang (1998) supports this surveillance argument and the importance of needing greater privacy protection in this age of database technology with his statement that “Data collection in cyberspace [has] produced data that are detailed, indexed to the individual, and permanent. Combine this with the fact that cyberspace makes data collection and analysis exponentially cheaper…and we have genuine threat of “dataveillance”” (1261).

Political scholar Colin Bennet (1996) describes this “dataveillance” as the surveillance practices that the massive collection and storage of vast quantities of personal data have facilitated. In doing so, he suggests that these database technologies enhance the potential of the government to intrude more easily on user privacy and argues for the growing importance of the privacy of one’s thoughts, property, location, and other entities that need protection with the emergence of these intrusive technologies. These scholars argue that, with the rise of database technologies, privacy should be framed as protecting an individual’s thoughts, property, location, and other entities from mass-surveillance of the government and therefore, of growing importance.
Yet, many privacy scholars disagree with the claims that fall under the “Big Brother” scenario. In other words, most disagree that a surveillance state will be created in the US as a result of these technologies, and that, for this reason, ensuring the privacy of an individual’s thoughts, property, location, and other entities is increasingly important. Solove (2004) argues that the data collection processes of these new database technologies have primarily not been orchestrated for surveillance purposes as the “Big Brother” metaphor suggests; instead, they have largely been ad hoc, arising primarily to use the data to better tailor products to the demands of the growing public and private sectors (Ibid). Moreover, many scholars emphasize that the goals of this data collection have often been benign rather than for mass government surveillance like the metaphor suggests (Ibid). Therefore, this scenario oversimplifies the importance of privacy with the rise of these new technologies since the scenario does not consider other factors, like innovation and convenience, that may be impacted if more stringent privacy measures were put in place.

‘The Trial’ scenario argues that the privacy implications of these technologies are not that they will be used in the US primarily for government surveillance purposes, but instead, are that these technologies will be used to study and exploit the individuality of the users of these technologies without the individual’s permission or awareness (Solove, 2004). Solove (2004) stated that these claims largely fit under the scenario name ‘The Trial’ because, like the main character in Franz Kafka’s The Trial, users of these technologies often have no say, no knowledge, and no ability to fight back about how their data is used or shared. The warning of legal scholar Michel Foucault (1977) fit into this metaphor that more recent data collecting technologies will have unintended, harmful social effects that may not be directly perceived by people. Foucault (1977) counters that rather than mass-surveillance this data collection will be harmful by possibly changing the landscape in which people act, leading toward an internalization of social norms that
soon is not even perceived as repressive as this surveillance is normalized. Like the Big Brother scenario, this scenario only focuses on the privacy implications of these technologies, and thus, also fails to consider the importance of other factors, like innovation and convenience, that individuals may value more than the privacy of their data collected by these technologies.

Moreover, while these privacy scenarios capture the general perception of the privacy implications of these new technologies, these scenarios are limited in their applicability due to their assessment of older technologies, like the first computers created, and their generalization of the frames and labels or perceptions of individual interpretive communities in society of the privacy implications of these technologies. The limited applicability of these scenarios to understanding current perceptions of privacy in the context of new technologies highlights how emergent technologies like wearables pose unique challenges to members of the privacy community, as well as new privacy implications.

2.3. DATA PRACTICES, PROCESSES, AND PROTECTIONS

Other evaluations of the privacy implications of these data collecting technologies have focused more narrowly on evaluating the potential of specific data practices, like data aggregation and data analysis to identify trends, to make these technologies more privacy intrusive and increasing the importance of data privacy protection for these technologies. Law professor Julie Cohen (2000) defines data aggregation as the idea that “[a] comprehensive collection about an individual [can be created that] is vastly more than the sum of its parts” (1398). Many scholars have expressed concern about the practices of data aggregation and data analysis to identify trends. For example, legal scholar Stan Karas (2002) expresses his concerns about these massive collections of individuals’ data because even non-taboo data like products consumed are expressive of an individual’s identity. For instance, such relatively ‘benign’ data can suggest what
Some evaluations of the privacy implications of these technologies have focused on the data practices of the processing and sharing of the data collected by these technologies and the potential for harm that errors in the bureaucratic processing and sharing of the data can have on an individual. Some privacy scholars, such as Julie Cohen (2000), are increasingly expressing concern that when the data collected by these technologies are processed, the data in these databases are often incomplete since “people are not simply reducible to the sum of their transactions, genetic markers, and other measurable attributes” (1405). Therefore, many of these scholars stress that the bureaucratic processing of these data could lead to these data collected being viewed as defining a person and being collected and shared without a person’s permission for purposes like screening the individual for a job application (e.g., Cohen 2000), suggesting the harm for the individual if the data in these databases is incorrect.

Existing bureaucratic processing of this data by companies and governments often does not allow the individual to participate in deciding how her data is collected and used. Even more, these databases or digital biographies are increasingly being accepted as truth and as providing the whole picture about an individual partially due to the efficiency of their use. In the 1960s, legal scholar Kenneth Karst (1996) first began warning about the risks of the centralized data processing systems of a growing number of technologies making the digital biographies easily accessible. Political theorist Jeffrey Rosen (2001) supports Karst’s concern about this growing overdependence on the use of these digital biographies. Rosen (2001) stresses that privacy needs to be taken into greater account to protect an individual from being mis-defined and judged out of context. Moreover, Rosen (2001) stresses that these digital biographies may contain errors or may
not portray the whole picture of the individual, leading to misinterpretation. As such, Solove (2004) states that privacy involves the power to refuse to be treated with bureaucratic indifference when one complains about errors or when one wants certain data expunged. Therefore, these scholars argue that the user’s lack of control over how this data is processed and shared is of most concern to them (Ibid).

In the case of both privacy metaphors and data-sharing practices, the problem of privacy risks prevails over divergent views among interpretive communities that may impact their value judgements and thus, their perception of privacy and the privacy implications of a new technology. These scenarios oversimplify the importance of privacy with the rise of these new technologies since these arguments do not consider the importance of other factors, like innovation and convenience, that may be impacted if more stringent privacy measures were put in place. Therefore, the limited applicability of these evaluations of specific data practices and processes to understand current perceptions of privacy in the context of new technologies highlights the importance of this thesis.

2.4. EXISTING US FEDERAL GOVERNMENT’S PRIVACY REGULATORY FRAMEWORK FOR WEARABLES

In recent years, scholars have focused on conducting legal analyses of the US federal government’s existing privacy regulatory and statutory frameworks in the context of the increasing use of more advanced, data collecting technologies, like wearables (Rubinstein, 2010; US Department of Health and Human Services, 2016; Banerjee, Hemphill, & Longstreet, 2018). For example, in June 2016, the US Department of Health and Human Services (HHS), which oversees Health Insurance Portability and Accountability Act (HIPAA) enforcement, released a report evaluating existing privacy oversight of health data collected by entities not regulated by HIPAA,
such as wearables (US Department of Health and Human Services, 2016). The HHS report determined that any wearable health technology used to manage or monitor an individual’s health not offered or provided by a covered entity or business associate is outside of HIPAA’s scope (Ibid.). The report notes that the technologies not in the scope of HIPAA may be subject to the jurisdiction of the FTC under the FTC Act (Ibid.) Moreover, the report states that due to this regulatory environment or lack thereof, the HHS has found that individuals and technology developers are confused or not aware of the regulatory requirements of these devices (US Department of Health and Human Services, 2016; US Department of Health and Human Services, 2014). The report clarifies that the FTC only has broad authority to enforce the FTC Act against for-profit entities engaging in unfair and deceptive acts or practices in or affecting commerce (15 U.S.C. § 45(a); US Department of Health and Human Services, 2016).

Legal scholars have found similar findings regarding the under-regulation of these recent, more advanced data collecting technologies (Rubinstein, 2010; Banerjee, Hemphill, & Longstreet, 2018). Much debate has arisen regarding the role of other kinds of oversight, like industry self-governance, and US values, like supporting innovation (Rubinstein, 2010). These factors are important to consider when evaluating, beyond a legal analysis, the current US federal privacy framework for wearables and its need to be modified (Ibid.).

2.5. OTHER TYPES OF OVERSIGHT AND US VALUES

With technologies like wearables relatively unregulated at the federal level, many scholars have tried to move beyond conducting legal analyses to argue for the role of different types of oversight. Some scholars have argued for and against the current effectiveness of industry self-governance when determining the need to increase federal privacy oversight for these technologies (Rubinstein, 2010; Solove, 2007; Solove, 2002). For example, legal scholar Ira Rubinstein (2010)
argues that “privacy self-regulation is a failure” because this type of oversight is ineffective without the necessary incentive structure in place to ensure wide scale industry engagement and to prevent ineffective compliance and enforcement mechanisms (355). At the same time, the Direct Marketing Association counters that the market is functioning optimally and is already adequately accounting for privacy concerns, suggesting its belief in the effectiveness of industry self-regulation in protecting user privacy (Webb, 2004). Moreover, legal scholar Nicolas Terry (2017) emphasizes the importance of privacy self-regulation by app stores and technology manufacturers in setting rules to ensure the privacy of the data collected by these under-regulated technologies. Economists Paul Rubin and Thomas Lenard further argue that privacy self-regulation by industry is effective since industry will put in place the consumer’s desired privacy policies to ensure that its reputation with consumers is not tarnished (Rubin & Lenard, 2002). Yet, some scholars counter that these privacy policies are not intended to be read by the consumer and while not deceptive, this notice-and-consent regime is not an effective approach at warning consumers of the privacy implications of using a technology (Rubinstein, 2010).

Some emphasize the importance of considering innovation and its potential to be inhibited by greater regulation when evaluating why increasing federal privacy regulation for these technologies may not be beneficial (Ibid.). For example, the Clinton Administration generally favored the view that the federal government should avoid imposing unnecessary restrictions on emerging technology sectors (Clinton & Gore, 1997). The Administration believed that regulation could distort market developments by “raising the cost of products and services” or by preventing US companies from keeping up with “the break-neck speed of change in technology” (Ibid.). However, these arguments for other types of oversight fail to analyze the different priorities of the
various interpretive communities holistically or to assess how the federal government should approach privacy moving forward to consider this privacy discourse.

2.6. HOW THE US FEDERAL GOVERNMENT SHOULD APPROACH PRIVACY FOR NEW TECHNOLOGIES

Arguments for other types of privacy oversight and US values have arisen during discussions about whether the current federal privacy framework needs to be modified moving forward. These discussions suggest that different perceptions of how and whether this framework should be modified exist between interpretive communities in the US privacy community. Scholars largely have reached a consensus that the existing federal level regulatory framework for privacy itself is insufficient in ensuring the privacy of the data collected by newer, data collecting technologies (Solove, 2004; Rubinstein, 2010). But only some scholars have proposed potential modifications to this framework. For example, legal scholar Ira Rubinstein (2010) suggests the potential of new models of privacy co-regulation based on insights from “second generation” environmental policy instruments like environmental covenants that move beyond voluntary codes (22). Other scholars have pointed to the models of other foreign governments, like the EU’s old data privacy directive, as models for US data privacy protection and have emphasized the need to use the privacy legal frameworks of these foreign governments as privacy models (Fromholtz, 2000; Barnes, 2006; McDermott, 2017). For example, Barnes (2006) recommends that the US enact a new federal privacy legislation that would serve as a baseline for data privacy, like in the EU, that would leave states to pass even more stringent privacy measures if they wish to. This recommendation recognizes that a handful of US states have led the way in strengthening consumer privacy protection and that federal privacy legislation should not preempt the progress on privacy legislation that many US states have made (Barnes, 2006; Ritter, Hayes, & Judy, 2001).
2.6.1. The Historic Role of the EU Privacy Perspective in the US Privacy Ecosystem

Privacy discussions in the literature generally have concentrated on assessing domestic US policy decisions with select scholars challenging this norm through adopting a comparative focus to understand the global privacy implications of other countries’ policy decisions, such as those of the EU (Schwartz, 2012; Bradford, 2012; Greenleaf, 2012; Newman, 2008). Scholars stress the historic role of the EU privacy model in influencing the US privacy model since the 1990s at the international data transfer level (Schwartz, 2012; Bradford, 2012; Greenleaf, 2012; Newman, 2008). Scholar Anu Bradford (2012) argues that the EU’s policy decisions have set the rules for privacy or ‘data protection’ globally, which she calls the ‘Brussels Effect’.

The EU has influenced the US privacy model through data transfer agreements between EU member states and the US, such as The European Commission’s 1995 Data Protection Directive (the Directive), which mandated in Article 25 that countries conducting data transfers with the EU have ‘adequate’ data protection (Directive, 1995; Determann, 2012). This ‘adequacy’ requirement resulted in the US and EU agreeing on the Safe Harbor, the two sets of Model Contractual Clauses, and the Binding Corporate Rules. Slaughter (2004) refers to this use of non-legislative lawmaking to cause other countries to work to adjust or harmonize their domestic law to continue cooperation with another country as “harmonization networks” (59). Other scholars point to the use of supranational privacy agreements before the 1995 Directive, such as the Privacy Guidelines of the Organisation for Economic Co-operation and Development (OECD) and the Convention on Privacy of the Council of Europe, that, although nonbinding, have influenced US international data transfer legislation (OECD, 1980; Schwartz, 2012, pp. 151-54). Schwartz (2013) attributes this ‘Brussels Effect’ to the EU’s importance as a global market that companies cannot
afford to lose and the growing dominance of the European Data Protection Supervisor (EDPS) in
the global privacy debate.

More recently, scholars have begun to discuss the anticipated and observed implications
of the GDPR, which seeks to establish de facto international benchmarks for corporate
information processing, on the US privacy policy frameworks at the US state and federal-levels
(Schwartz, 2013; Del Pizzo, 2019). US-based media and scholars suggest the GDPR’s influence
on the CCPA, which the state passed on June 28, 2018 and will become operative January 1,
2020 (de la Torre, 2018; Del Pizzo, 2019). CCPA parallels the GDPR through its provisions that
allow consumers to demand businesses to disclose personal information that they collect on
them, to stop companies from selling their personal information, and to understand how
businesses store and share their data (CCPA, 2018). In September and October 2018, the Senate
Commerce Committee raised in a hearing with multiple large tech companies the GDPR as a
privacy model and highlighted that the hearing would discuss possible approaches to
safeguarding privacy more effectively (United States, 2019). This sentiment was captured by
Senator John Thune (2018) of South Dakota’s statement that

On June 28th, the California Consumer Privacy Act was signed into law. Like GDPR, the
new California law—which will take effect on January 1, 2020—contains many privacy
mandates and severe penalties for violators…The question is no longer whether we need
a federal law to protect consumers’ privacy. The question is what shape that law should
take.

Partially as a result of the GDPR going into effect on May 25, 2018 and the desire of tech
companies to preempt the CCPA with a federal privacy legal framework, at the end of 2018, some
large tech companies have pushed for the adoption of a federal framework (Intel, 2018). Some
reports note that companies seem more willing to adopt a GDPR-like federal framework since
many companies have already adopted the GDPR principles and applied these protections to all
their consumers. For example, in September, Microsoft announced that the company had extended many of its GDPR protections to all its customers (Brill, 2018).

Yet, in the literature, very few written articles exist that discuss the implications of GDPR on the US privacy model, partially due to the regulation’s new nature, or, more specifically, whether the EU’s privacy framework serves as a better model than the US’s for wearables (SEE TABLE 2). Discussions surrounding the GDPR’s impact on wearables primarily are found in forms, such as: newspaper articles (Baxter, 2017) and wearables-focused websites (Charara, 2018). Therefore, the thesis includes a brief sub-analysis of interviews from a small group of European Commission officials to highlight any similarities or differences between the EU and US perspectives on privacy for wearables and to better put into context EU perspectives on privacy that may have been raised by US interpretive communities. Moreover, this analysis of the transcripts of these European Commission-level officials provides a value point of comparison, regarding similarities and differences in how EU and US communities frame privacy and evaluate their privacy framework for wearables.
SECTION 3: THEORY AND METHODOLOGY

3.1. INTERPRETIVE POLICY ANALYSIS

Currently, the US does not have a consensus across its policy-relevant actors on the issue of how data privacy should be protected for wearables. The qualitative, interpretive policy analysis methodology introduced by Dvora Yanow (2000) was applied to uncover labels and frames used by different policy-relevant actors. Interpretive policy analysis serves to comprehend what policies and practices mean to different interpretive communities affected by them such as policymakers, implementing agency personnel, and affected citizens (Yanow, 2000). In the context of this thesis, interpretive policy analysis is used to answer through semi-structured interviews the following questions: How is privacy labeled and framed by policy-relevant interpretive communities in the US? How does this relate to their evaluation of the existing US federal government's privacy regulatory framework for wearables? How does this relate to their perception of how the US federal government should approach data privacy for these technologies moving forward? A total of 33 individuals were interviewed for this thesis. 27 subjects were interviewed from the US communities, and 6 subjects were interviewed from the EU government community.

Rather than assuming that policy discourse is objectively rational or factual in nature, this thesis maps out how interpretive communities frame policy-issues differently and possible explanations for why (Yanow, 2000). These communities are referred to as ‘interpretive communities’ since group processes have stimulated the members to share similar thoughts, speech, practice, and meanings to talk about ideas and action (Ibid). Yanow (2000) identifies five steps to interpretive policy analysis (SEE FIGURE 1), which are used in this thesis as a research design framework. The first step is to identify the artifacts (symbolic language, symbolic objects, symbolic acts) that are significant bearers of meaning (values, beliefs, feelings) for a certain policy-
issue, as perceived by interpretive communities and policy relevant actors. The second step is to identify the interpretive policy-issue relevant communities which create or interpret the artifacts and meanings. The third step is to identify the community discourse of each interpretive community around the policy-issue. The fourth step consists of identifying the meanings that are in conflict between or among groups and their conceptual sources (affective, cognitive, and/or moral). The fifth step is then to analyze the implications of these different meanings across interpretive communities for policymakers. With this methodology, it is important to note that the first two steps of the interpretive policy analysis can lead to each other, and steps 1, 2, and 3 are usually done at the same time (explained in detail in Yanow, 2000).

![Steps of conducting an interpretive policy analysis - posed by Dvora Yanow (2000)](image)

**Figure 1.** Steps of conducting an interpretive policy analysis - posed by Dvora Yanow (2000)

3.2. **RESEARCH DESIGN**

First, this thesis uses Solove’s (2002) broad definition of “privacy” (67):

"Privacy" is a general term that refers to the practices we want to protect and to the protections against disruptions to these practices...we should conceptualize privacy by focusing on the specific types of disruption and the specific practices disrupted.

This definition was chosen over others because it recognizes the ambiguous nature of the term “privacy”. This definition recognizes that how privacy is defined depends on social practices,
activities, customs, and norms that are shaped by history and culture (Solove, 2002). Therefore, this thesis uses this definition as a reference, and through document analysis, explores how this term is defined by different interpretive actors and how its meaning is contested by actors using other framings of privacy. Second, this thesis applies this framing through the interpretive policy analysis method introduced by Yanow (2000). An interpretive policy analysis is useful for this type of thesis since the analysis is based on philosophical presuppositions that emphasize a context-specific meaning system and the meaning system-based understanding of social realities.

**STEPS 1 & 2: IDENTIFY ARTIFACTS & THEIR MEANING & IDENTIFY THE INTERPRETIVE COMMUNITIES**

The first step of the analysis is to identify artifacts and the meaning attached to them with regard to symbolic language. Yanow (2000) offers two methods to discover meaning accorded to a policy-issue: metaphor and category analysis. To uncover a metaphor in policy language and acts and to uncover its meaning for the actor or agency within their frame of reference helps to understand the structure of the policy argument (Ibid.). Therefore, this thesis uses metaphors to uncover how different policy-issues are defined, perceived, and evaluated by various interpretive communities.

The analysis involves a description of actors in the different interpretive communities and presentation of their 1) framing and labeling of privacy, and 2) framing of the policy-issue of privacy for wearables. This framing includes providing an outline of the artifacts or symbolic objects of each organization that each actor in the community interviewed represents. It also includes the organizational structure and the size of the organization that each interview subject belongs, which is identified through analyzing websites and reports of the organization that the subject represents, if possible. Determining this framing begins with an analysis of the symbolic
acts that can impact the meaning or perception that an interpretive actor has towards a policy issue. With regard to symbolic acts, this method involves looking for meanings inherent in: first, acts of legislation, holding of hearings, views on the matter, and the omission of any of these acts, and second, in the comparison between acts and words (Ibid.).

Of the three analytic categories, analyzing symbolic acts can be the most complicated, because they are the least visible to an outsider and accessing communities to uncover their meanings takes large amounts of time and effort (Ibid.). Due to time constraints, meetings were not attended to uncover meaning in the actual implemented policy programs as the investigator did not get the chance to visit the organizations’ working areas. However, the thesis does analyze the policy programs and policies the policy-relevant actors in each interpretive community have implemented and those that are currently running. To uncover potential influences on these organizations, donors to each organization in the different interpretive communities are assessed, provided this information is available.

This thesis identifies the policy-relevant interpretive communities through analyzing the primary interpretive communities in the US privacy community that are relevant for the US privacy policy-making process. The three US interpretive communities include: the US federal government, the private sector, and public interest groups. In my analysis, the public interest groups community is divided into two sub-groups: pro-industry and pro-consumer protection.

The interpretive communities selected are in no way inclusive of all stakeholders in US policy-making process since there are so many different stakeholders. Public interest group refers to “an organizational entity that purports to represent very broad, diffuse, non-commercial interests which traditionally have received little explicit or direct representation in the processes by which agencies, courts, and legislatures make public policy” (Schuck, 1977, pp. 133). The private sector
refers to the companies and law firms that advise and lobby for companies to government on privacy issues (Rudder et al., 2008).

In addition, for comparison purposes, the thesis analyzes interview transcripts from an interpretive community, consisting of European Commission-level officials, regarding its framing of privacy and its evaluation of the Commission’s privacy framework for wearables. This community refers to those individuals working for the EU government in an official or advisory capacity.

**STEP 3: IDENTIFY COMMUNITY DISCOURSE**

For the third step of the analysis, this thesis identifies the discourse between the US and EU interpretive communities through conducting document analysis and analyzing the transcripts from the semi-structured interviews with the interpretive policy-relevant communities. To complete the third step of the analysis, the transcripts of the policy-relevant actors interviewed are analyzed using the creation of a coding scheme to identify the community discourse between the different communities and to determine the framing and labeling of privacy by these communities (SEE TABLES 1, 3, & 4). This section focuses on drawing from the transcripts of the actors in the communities assessed to present each interpretive community’s discourse.

Based on an analysis of the interview transcripts, section three is divided into four subsections with each subsection focusing on analyzing the different responses regarding the following three thematic concepts of the questions that were asked:

1. Framing privacy;
2. Evaluation of the existing US federal privacy framework for wearables;
3. Perceptions of moving forward
4. EU analysis – Comparison of EU perspective
Each of the above thematic concepts focuses on presenting 1) how different communities label and frame privacy; 2) how each community evaluates the existing US federal government's privacy regulatory framework for protecting data privacy for wearables; and 3) how each community perceives how the government should approach privacy for these technologies. These privacy framings, evaluations, and perceptions are determined based on an analysis of the language and behavior used by the actors in each community according to their interview transcript. The language and behavior used will present the meanings or conceptual sources -affective, cognitive, and/or moral (corresponding to feelings, values and beliefs)- of each interpretive community.

**STEP 4: IDENTIFY THE CONFLICTING MEANINGS WITHIN OR BETWEEN GROUPS**

To complete the fourth step of the analysis, this thesis will analyze and compare the privacy framings, evaluations, and perceptions of the different interpretive policy-relevant communities. These comparisons will focus on the communities’ evaluations of the existing US federal government's privacy regulatory framework for protecting data privacy for wearables and their perceptions of how the US federal government should approach privacy for these technologies moving forward. Section 4.4 will analyze, for comparison purposes, transcripts from interviews with European Commission officials to highlight the uniqueness of US privacy perspectives and identify US communities that may share aspects of the EU privacy perspective.

**INCLUSION CRITERIA**

To be selected to be interviewed, the inclusion criteria was that the subjects had to fall into one of the following categories: a current or former EU official that works or has worked with issues related directly or indirectly to wearables' or privacy legislation; a current or former US government official that works or has worked with issues related directly or indirectly to
wearables’ or privacy legislation; a current or former US private sector employee that works or has worked directly or indirectly with wearables technology or privacy legislation, including at a public interest group, a law firm advising or lobbying for businesses, or a business.

**DATA COLLECTION**

The snowball networking approach was used to select individuals to interview (Yanow, 2009; Wong & Sharp, 2009). The initial interviews in the US were arranged through email requests being sent to the general email addresses listed on the FTC’s website and to the specific email addresses of privacy experts at public interest groups, companies, and various US universities available on the organizations’ websites. The initial interviews in the EU were arranged through email requests being sent to the general emails of EU directorates and the EU Data Commissioner listed on the European Commission’s website.

Interview responses were collected after using Georgetown University Institutional Review Board (IRB)-approved questions when interviewing subjects. These questions fall into three primary categories: 1. The subject’s perception of the privacy risks of wearables and the importance of privacy protection with the use of these technologies; 2. The subject’s perception of what the characteristics of the existing (US federal or European Commission) regulatory framework for privacy for wearables are; 3. The subject’s evaluation of the strengths and weaknesses of using the existing privacy regulatory framework for wearables; 4. The subject’s perception of the future outlook of (the US or the European Commission’s) privacy regulation and the subject’s perception of how (the US or the European Commission) should approach privacy for these wearables moving forward.
SECTION 4: RESEARCH FINDINGS

In Yanow (2000)’s conceptual framework of interpretive policy analysis (SEE FIGURE 1), the policy analyst draws connections between the beliefs, feelings, and values of those involved in the policy landscape. Themes of both consensus and divergence emerge from the questions asked. This section focuses on analyzing interview transcripts across interpretative communities to compare responses in the following categories: 1. Framing privacy; 2. Evaluation of existing US federal privacy framework for wearables; and 3. Perceptions of moving forward. Section 4.4 analyzes transcripts from interviews with officials from the European Commission to highlight the uniqueness of US privacy perspectives and identify US communities that may share aspects of the EU privacy perspective.

4.1. FRAMING PRIVACY

This section bases its analysis on three questions that sought to capture the symbolic words and narratives that the interpretive communities used to: define their interpretation of the value of privacy for wearables (1. How data can be used; and 2. With whom should this data be shared); discuss the value of privacy for wearables based on the privacy risks they pose; and assess the value of privacy in comparison to other factors. To analyze how the communities assessed compare in these theme areas, this thesis analyzed responses to the following interview questions:

1. Do you think that there is any privacy risk associated with lifestyle and wellness wearable technologies?

2. Can you give me examples of what might be a risk and what might not be a risk of this technology? What influenced your thinking about this risk?

3. What would you say are the primary characteristics of this US approach to ensuring the privacy of the data collected by these wearable technologies?
**4.1.1. HOW DATA CAN BE USED**

Across communities, a shared definition of privacy emerged around a common sentiment that privacy refers to a user’s awareness of the types of information that can be collected, accumulated, and combined with other information about him/her. A review of the interview data noted that 27 of the 27 US interviewees (100%) used key words that fall under the ‘User Awareness of Data Use’ code when responding to questions. Subjects often referred to the importance of a user being aware of how their data is being utilized, when describing what privacy means to them to better explain their perception of the privacy risks of the technology. A senior policy analyst in the pro-consumer protection community conveyed this sentiment through pointing to the use of privacy policies by companies as an example of when privacy is not maintained through her statement that: “A terms of service statement really doesn’t capture people’s perceptions of what privacy is. I don’t think most people believe that people read terms of service, I don’t think that we can in any sort of good faith expect people to understand the types of information that can be collected, accumulated, sort of combined with other sets of information,” suggesting this association of privacy with a user being aware of how her data is collected and used.

The pro-consumer protection public interest group expanded on this definition by including in its framing of privacy, the importance of a user providing informed consent before their data is used. For example, if an individual wears a wearable device to track her step count and blood pressure, she should be made aware of how her data is being collected and used, and additionally should be asked to provide informed consent before her data is used. ‘Informed consent’ refers to the concept that an individual using a technology is fully aware of how their data is being processed by a company and consents to this data collection and use. A review of the interview data noted that 100%, or 5 of the 5 interviewees, in the pro-consumer protection community used key words
that fall in the ‘Informed Consent of Data Use’ code when responding to questions. Symbolic
language, including: “right” and “choice”, emerged as common words used by individuals in this
community to convey this concept of informed consent as an important facet of their definition of
privacy. A senior policy analyst at a pro-consumer protection public interest group conveyed this
sentiment through his reference to Warren and Brandeis’s (1980) concept of the “right to be left
alone” when explaining his framing of privacy. He supported this concept of informed consent as
an essential component of privacy and, similar to others in this group, referred to privacy as a
‘right’ through his statement that:

Privacy is the right to not be exposed in ways that you don’t want to be exposed and not be
monitored…your sort of right to control how you are exposed and how you’re dealt with
and whether your data works…you know you’re right to be left alone.

Individuals in this pro-consumer protection community stressed that an essential aspect of
privacy is that users provide consent to how their data is used since they have a right to privacy.
Many subjects explained that individuals desire privacy and expect that their privacy will be
protected: “…if you do not want to be photographed, you believe that you will not be
photographed”, which suggests his perception that users generally want to be aware when a
technology is collecting data on them and to provide consent before this data is collected or used.
In framing the importance of informed consent to ensuring an individual’s privacy, this group often
made references to the EU’s designation of the fundamental human right to privacy to point to a
similar interpretation of what privacy is.

4.1.2. WITH WHOM SHOULD THE DATA BE SHARED

When framing the risks of these technologies, the communities diverged in their framing
of the importance of privacy in data sharing. This thesis acknowledges that data can be shared in
four ways: through illicit means (i.e. a hack) to transfer data to a malicious actor, through legal
means from the user to another actor with the data owner’s informed consent, through legal means between a company to a third party with the informed consent of the data owner, and the data being transferred to a third party without the informed consent of the data owner.

When discussing the privacy risks of wearables, the US communities shared a sentiment that data should never be transferred illicitly, such as through a hack, or legally to malicious actors. 19 of the 27 transcripts analyzed fell into the ‘No Data Sharing to Malicious Actors’ code when discussing who should be shared the data collected by a wearable.

As a result, many subjects emphasized the importance of ensuring that the device has strong cybersecurity to ensure that the user’s privacy is not infringed upon by a malicious actor being shared the data. The US communities suggested the importance of ensuring privacy from malicious actors through the use of terminology including: “data breach laws,” “encryption,” and “passwords” when discussing examples of actions that companies can take to ensure user privacy for their devices. Moreover, many subjects interviewed used terminology, such as: “hacking” and “stealing data,” when framing the privacy risks associated with these technologies, suggesting their perception that to ensure user privacy, malicious actors should not be shared this data.

A senior US government official conveyed this sentiment through his explanation of how privacy may be less protected in other countries and his suggestion that a data hack infringes upon an individual’s data privacy:

You are more likely to see countries—China being one example—where hacking businesses and taking data and not having kind of either ethical standards or repercussions within their own legal system for doing so, puts people’s privacy at risk in a way we couldn't imagine. Kind of the scenario I'm imagining is that I could imagine Chinese hackers stealing data from companies and using it to kind of fuel AI systems, for example, just to get the raw data, which is something I'm sure a lot of companies would love to do, but you know won't see happen in the US because it’s ethically dishonest and would put them through a lot of legal exposure.
The pro-consumer protection public interest group community expanded on this interpretation of who should not be shared this data to ensure a user’s privacy by acknowledging the importance of data not being shared to a third party without the user’s informed consent. This sentiment is suggested by 80% of the responses (4 of the 5 transcripts) from this community falling into the code category ‘Shared with the User’s Informed Consent’. A senior policy analyst suggested the value of providing informed consent in ensuring an individual’s privacy when a company shares data to a third party through her statement: “…imagine a scenario where information that someone you know didn't want to be shared ended up getting shared or, in some abstract way, someone's privacy rights were violated”. An assistant policy advisor conveyed the importance of neither malicious actors nor third parties being shared a user’s data through his statement:

There are two elements of privacy. One is the concept of individual autonomy…that individuals have a space where they can control the knowledge about themselves and that is things like: I grant consent for you to use the data from my college education. That's an example of something which can be controlled from a perspective of individual autonomy. The other is fair processing and that means the data is being used and shared in a fashion that is fair to the user of the technology who is having their data collected.

4.1.3. VALUE OF PRIVACY BASED ON PERCEPTION OF PRIVACY RISKS OF WEARABLES

This section analyzes each community’s valuation of privacy based on their perception of the privacy risks of wearables. Based on an analysis of the interview transcripts, this thesis identified: type of data and use of data, as themes that emerged when communities discussed factors that impact their perception of the privacy risks of the data, and, therefore, the value of privacy being maintained.

4.1.3.1. TYPE OF DATA
Communities shared a consensus that the value of privacy for wearables depends on the type of data being collected. 100% of individuals or 27 of the 27 transcripts interviewed used terms related to the code for ‘Type of Data,’ when framing the privacy risks of wearable technologies and for what type of data, they perceive that a user should have privacy protection for.

The communities referred to location data and data combined from several measurements or ‘aggregated data’ as the types of data that posed the greatest risk to privacy. Generally, subjects interviewed did not value privacy as much for types of data, such as heartrate or blood pressure measurements. The director of privacy for a pro-consumer protection public interest group expressed her reduced concern for individual data points through her explanation that:

There’s definitely a really wide range of data that you can gather from these devices and I do think that some classes of it are potentially very personally revealing. That said, I think there are a few different scenarios that start to make things both interesting and complicated. One is that, again you know, a lot of these things that Fitbit and Apple watches and things collect: any one item is probably not very risky but they're more risky in combination with other kinds of data that you might provide...so I think you could look at things like, you know, heartrate and fitness and movement in a similar way that it's not maybe just those pieces independently, but it's the value that gets added as other things are inferred about you that makes privacy for wearables important.

Many interview subjects justified their stance on the importance of privacy for certain types of data over others through references to their sensitivity and the consequences of the data being shared. Some individuals stated risks of more sensitive data, including: discrimination based on health condition, targeted advertising, and law enforcement tracking. A policy advisor from a pro-consumer protection public interest group pointed to the potential of discrimination based on health data that can result from analysis based on aggregated data about the individual. He explained this risk and the importance of privacy for this data in his statement that:

People say that “I don't care if someone else sees my heartrate information”—but many of the newer applications are getting very specific kinds of information. Because of a medical risk that you have, you decide to check other metrics about your medical condition, the knowledge of that can put you at risk for discrimination if someone gets a hold of that
information and wants to identify people with, for example, a certain HIV status. This could put you at risk for employment. This could put you at risk for insurance.

The vice president of software development and design at a smaller wearables company emphasized the value of privacy for sensitive data, such as location data, in protecting against the risk of targeted advertising through his explanation that:

Every person is essentially trackable, and it doesn't take many algorithms to push a coupon as they're walking by a store. That is being done, not by proximity like a Bluetooth pairing or a simple signal between the two parties, but, instead, is being done at a macro level with the information collected on a person and pushed through the cloud.

When discussing the sensitivity of location data, many subjects referenced the ease of reidentifying an individual based on their location, with multiple subjects referring to the findings of the *Nature* article “Unique in the Crowd: The privacy bounds of human mobility” (de Montjoye *et al.*, 2013). An analysis of the transcripts showed that 6 of the 27 interviewed from the US communities referred indirectly to this article. A senior policy advisor referred to the article in conveying the ease of reidentification through this location data through his statement: “Well, there's a paper out there that shows that you only need like four cell sites location to uniquely identify a person because there just aren't that many people who cross through the same four cell towers in a given day so you know.” In this article, de Montjoye *et al.* (2013) conclude that deidentification of data by companies does not ensure a user’s privacy, since four spatio-temporal points or four location points are enough to uniquely identify 95% of the individuals.

Other subjects raised concern regarding the privacy risk associated with location data through enabling targeted advertising and law-enforcement tracking. A software developer from the private sector community conveyed his concern regarding this geo-tracking through a narrative about the privacy risk of geo-tracking enabling easier targeted advertising; the narrative described an individual walking down the street and being targeted by advertising. He explained that an
individual can either be targeted by advertising through a signal being sent to the individual’s phone whenever they are near a store that makes an advertisement pop up; or by tracking at the cloud level, which makes an advertisement be sent to users whenever their geo-coordinates nears a certain location. A senior advisor for software development and design at a smaller wearables company stressed the privacy risk of this aggregated data being used for law enforcement tracking through his statement that:

I think that one area that is undervalued right now is location tracking, and I think that that's a big can of worms that has been underestimated significantly because if I'm being monitored for health it's one thing to count my steps, it's another thing to have my location at every point in time tracked because that opens up a whole can of worms relative to law enforcement. The data records that are being gathered aren't just being used by the company to augment the rationale for which you bought the product, but also to provide secondary services and potentially be used by the government or anybody else for any purpose.

4.1.3.2. USE OF DATA

Moreover, the US communities agreed in their responses that the value of privacy for these technologies depends, as well, on how the data is going to be used. All but one of the individuals interviewed used terms related to the code for ‘Use of Data,’ when framing the privacy risks of wearable technologies and for what type of data, they perceive that a user should have privacy protection for. Many individuals expressed the greatest concern about data aggregation due to their consensus that data analyzed is increasingly being processed to make assumptions about people and people’s mental state in the future. A representative in the pro-industry public interest group framed his concern about future technologies advancing with a narrative about his colleague’s attempt to game a mental health application that determined through “smart thinking” that his colleague was lying to the app after noticing that the user’s location was changing too frequently for someone that would be depressed. A director of business development at a larger technology company in the US stated that “…technology is collecting lots of data on all of us and they will
collect more. The better they get at collecting information, it will be harder to maintain privacy…,” suggesting her belief that privacy will become increasingly important, but harder to maintain, as more data continues to be collected on individuals.

4.1.4. IMPORTANCE OF ENSURING INNOVATION WHEN WEIGHING VALUE OF PRIVACY FOR WEARABLES

When weighing the value of privacy for wearables, innovation emerged as an important other factor that US interpretive communities raised. An analysis of the interview transcripts found that the word ‘innovation’ occurred 54 times and 100% of subjects from the US communities referred to terms related to the ‘Importance of Innovation’ code at least once in their transcripts. The US communities suggested this sentiment through their emphasis on the importance of not restricting the data flows in any way, unless the data is sensitive, so as to not restrict innovation. A former privacy researcher at Intel shared a document, highlighting the company’s position on privacy as of November 2018, which suggests that privacy protection needs to be weighed with other values: “What the US needs is a privacy law that parallels the country’s ethos of freedom, innovation and entrepreneurship” (Intel, 2018). A former private sector wearables researcher conveyed a similar sentiment through his statement that:

There really haven’t been instances that we have identified data actually used to generate any kind of harm. So, they are still almost entirely theoretical. So, on the one hand, I want to say protecting people’s privacy is important, but, on the other hand, I want to be a good Bayesian and say—yeah, but the probability of that bad outcome is very low, so I don’t want to require a bunch of regulation and protections to protect against something that probably isn’t going to happen. What I’m concerned about is how does the law adapt over time and if it does not have the capacity to adapt at all a little and fast enough.”, suggesting the belief that protecting innovation must be weighed with consumer privacy protection since regulation lags behind technological advancement and could hinder innovation.

Other subjects conveyed their favoring of innovation over privacy through acknowledgements that privacy will have to be reduced in an increasingly observational world to
allow the continued development of these technologies. A senior developer at a wearables company expressed this preference for innovation through his statement that:

Autonomy will decrease because of this increasingly observational tech world that needs sensors everywhere to make decisions. The future will be hindered by the controversial-ludicrous-idea that individuals view that we have “the right” to have control over all collection and use of data in an observational world that needs to monitor you to operate.”

Moreover, subjects referred to the FTC’s decision at two hearings in 1996 and 1997 to not restrict the use of cookies by companies to stress that the US has made a conscious decision to not hinder innovation for new technologies through privacy regulations (FTC, 1998). Reiterating their belief in the value of innovation, the US communities often cited this inadequate privacy protection as having been beneficial for providing the US an advantage over other countries. This sentiment suggests that, although these communities shared a consensus of what data should be used and who the data should be shared with to ensure a user’s privacy, other factors, such as innovation, may influence a community’s evaluation of the need for privacy regulations, especially if the regulations may hinder innovation.

Subjects further stressed the immense value of innovation in comparison to privacy through their association of innovation with ensuring economic security and, ultimately, protecting US national security. Subjects, particularly in the private sector, pro-industry public interest group, and US government communities, often referred to the competition between the US and China to be the most advanced in emerging technologies to stress the importance of the US government not inhibiting the ability of US companies to innovate. In particular, these communities raised the importance of considering innovation when deciding whether to restrict information flows to improve consumer privacy protection if these restrictions would inhibit the ability of US companies to dominate in emerging technology areas, such as machine learning and artificial intelligence. Subjects interviewed from the US government community reiterated the importance
of ensuring US innovation, the free flow of information for research, and that privacy regulation
does not create “roadblocks for innovation.” A former US government official conveyed the
importance of not restricting US innovation through his statement that:

You know sometimes having perfect privacy, where no one gets to access any of the data,
is not necessarily a good outcome, right? So, it might be a good outcome for privacy, but, in reality, if say we’re getting a lot of rich health data or maybe some of these health data
and wellness data have, you know, implications for public health…if those data are never
seen by anyone because of privacy interest—because there might be some privacy risk—we
may be losing some of the benefit. Policies need to balance these things—privacy is one
thing that we want, but there are other benefits in society that we could get by coming up
with responsible ways to share information and enabling innovative uses of the data.

The US communities raised other factors to be considered when weighing the value of
privacy, including: protecting freedom of expression and freedom of press, which can often limit
an individual’s privacy. However, during an analysis of the interview transcripts, these factors did
not emerge consistently within communities or across communities as a factor that subjects
considered important when weighing the value of privacy.

The greatest degree of consensus occurred when discussing other factors to consider when
assessing the value of privacy, with all communities identifying innovation. The private sector, the
US government, and the pro-industry public interest groups shared the greatest amount of
consensus and the sentiment of the pro-consumer protection public interest groups diverged the
greatest from the other communities. This divergence primarily emerged as a result of this
community’s focus on the user providing informed consent when her/his data is used or shared.

The importance placed on innovation by these communities suggests that they consider
other factors in society when evaluating privacy policies and whether privacy protection under
these policies should be modified. For example, if innovation is valued more in society than
privacy, then this society should have fewer privacy regulations in place that could restrict
innovation. Although these communities may share similar definitions of privacy, different
valuations of factors, such as innovation, when weighing the value and meaning of privacy to them resulted in differences in their perceptions of the need for privacy regulation.

4.2. EVALUATION OF EXISTING US FEDERAL PRIVACY FRAMEWORK FOR WEARABLES

This section bases its analysis on four questions that sought to capture the symbolic words and narratives that the interpretive communities used to convey their evaluation of the existing US federal government’s privacy framework for wearables. The themes that emerged in this section parallel each community’s initial framing of the value of privacy to them and other factors that they consider when weighing the value of privacy. To analyze how the communities assessed compare in these theme areas, this thesis analyzed responses to the following interview questions:

1. What do you consider the US’s approach to ensuring the privacy of the data collected by lifestyle and wellness wearable technologies?
2. In your opinion, what do you think are the strengths and weaknesses of this approach of the federal government to ensuring the privacy of the data collected by this technology?
3. What do you think have been the biggest influences on this US approach to privacy and its characteristics?
4. How do you think that the US’s approach to privacy compares to that of other countries in ensuring the privacy of the data collected by wearables?

4.2.1. INADEQUACY OF EXISTING FEDERAL FRAMEWORK IN PROTECTING PRIVACY

Across interpretive communities, consensus was found that the US federal government’s current privacy framework for wearables is inadequate itself in protecting a user’s data privacy.
19 of the 27 interviewed from the US communities referred to terms related to the ‘Inadequacy of Existing US Framework’ code at least once in their transcript. Although asked about strengths of the existing framework in protecting privacy, the communities often focused on the weaknesses of this framework in protecting consumer privacy. Subjects used a comparison to HIPAA and its stronger privacy protections to convey their evaluation of the insufficient nature of the US’s current privacy framework for wearables. Common language used to evaluate the privacy framework included: “inadequate”, “the wild west”, and “not well-designed”. One subject from the pro-consumer protection public interest group described the framework as “profoundly broken” and attributed this to the “US policy tend[ing] to favor the business, economic interests rather than the privacy interests of the individual”.

4.2.1. NOTICE AND CONSENT REGIME

Subjects across communities expressed their perception that the US’s notice and consent regime for privacy does not align with how people think and how technology is evolving and is a weakness of the current US framework in protecting consumer privacy. A software developer from the private sector community conveyed the technical flaws of the notice and consent regime in the US:

I think in terms of like what needs to change… I think that we need to reevaluate the current notice and consent system in place in the US... We haven't figured out good ways of providing notice and consent for these wearable devices... these are not the same thing as websites and computers, they don't have the same types of interfaces. They don't-some of them don't even have screens or screens that can convey a lot of information, let alone a four or five-thousand-word privacy policy of some kind. That's a really basic problem here. I don't know that there's a good regulatory solution to solving it, but it's something that needs to be rethought.

4.2.1.2. EXPLOITATIVE BUSINESS MODELS HAVE EMERGED

Subjects across the US communities expressed consensus in their perception of the risk of this underregulated framework in negatively impacting consumer privacy protection through
enabling potentially exploitative business models emerging based on the use of this data. This sentiment regarding the weakness of this framework in enabling these exploitative business models connects with the consensus across communities in their framing of privacy regarding their concern about the use of data aggregation and the use of data aggregation in the future. One privacy researcher from the pro-consumer protection public interest group community captured this perception with her statement that:

> Often people have no choice but to give up their data if they want to use a technology. Is it feasible to not use these technologies in today's connected world? The policies put the onerous burden on the consumer to make decisions regarding their privacy protection when often consumers aren't thinking about the future and the use of their data...unless they are a privacy expert, that is.

Another privacy researcher from the pro-consumer protection public interest group community captured this perception with his statement that:

> I would say one of the interesting things I have found from my own research is that there is an assumption by a lot of the public that there are laws that protect them that don't actually exist, and I think that in the health space this is doubly true than compared to, let's say online searches—searches with Google or another search provider.

### 4.2.1.3. WEAK FEDERAL TRADE COMMISSION ENFORCEMENT CAPABILITY

The US communities expressed consensus in their perception that, in terms of protecting consumer privacy, the US’s current privacy framework for wearables is inadequate as a result of: the inability of the FTC to impose large fines on companies that disregard consumer privacy, the under resourcing of the FTC, and the FTC’s lack of rule-making authority. A senior policy analyst from the pro-consumer protection public interest group captured this perception through her statement that: “The FTC can make a company’s life difficult through an enforcement action that forces them to comply with a level of monitoring and restrictions on their business practices that’s just not the same as being hit with a three billion dollar fine. That would make a big difference.”
A senior privacy researcher from the pro-consumer protection public interest group captured this perception with her statement that:

I mean the FTC can't pass regulation or is, you know, limited in how it can pass regulation. It's limited, I think, in terms of kind of its ability to fine companies. I mean one of the biggest improvements with the GDPR is the fact that when a company is accused or proven to violate the GDPR, the European authorities can fine it. I don't know what the percentage is, but I mean basically their fines can amount to like billions of dollars against an entity like Google and at that amount companies take notice, you know? Whereas, when there's a 20 million dollar enforcement action, which is what I think Uber was slapped with not long ago, it's not an insignificant amount of money, but they can pretty much just take it and keep on going…so I think the FTC's ability to levy fines needs to be improved certainly in both the amount and their capacity for doing so because a twenty million dollar fine on a Google is just like…they probably make that in an hour. It's fairly insignificant.

A former official from the US government community expressed a similar sentiment with his statement that:

The FTC is understaffed and cannot make a business go out of business and cannot fine on the first offense, which are big weaknesses. Really, it does not have necessarily the expertise or the tools to deal with the issues that we're seeing, and, certainly, when it does in fact go after companies, we've seen kind of time and again that even when it does censure companies they either ignore it or they find ways around it.

4.2.1.4. DIFFICULTY OF QUANTIFYING HARMS FOR LEGAL PURPOSES

The US communities expressed consensus in their perception that in solely focusing on whether the framework protects consumer privacy, the framework is ineffective or inadequate. They emphasized that the FTC Act’s Unfair and Deceptive Practices effectiveness depends on the ease of determining the harms incurred by the consumer, which is often very difficult to determine or prove in today’s privacy context. One subject from the pro-consumer protection public interest group captured this perception with her statement that:

There’s a focus on trying to prove harm, where I think a lot of the risks and the issues we face today aren’t or can’t be reduced to simple questions of: did you experience financial harm or embarrassment?...or something that looks like a privacy tort. Whereas in the EU, privacy is defined as both a right and a dignitary interest, so you don’t have to define a threat to privacy as just a harm.
A senior privacy researcher from the pro-industry public interest group reiterated this perception with his narrative of his recent work, which focused on providing the US government with his evaluation of the FTC’s effectiveness in protecting consumer privacy. He highlighted his evaluation of the framework’s inadequacy through his statement that:

Earlier today, I actually spoke with someone about the strengths and weaknesses of the existing privacy regulatory framework under the FTC. The FTC currently has enforcement jurisdiction, and I was asked by the administration how FTC should change because currently there is only in place the unfair and deceptive practices enforcement under the FTC Act. However, to make something unfair so that it falls under the FTC Act, there has to be empirical evidence of harm, but this doesn’t consider idea of unconsidered harms, like embarrassment.

4.2.2. STRENGTH: FEDERAL FRAMEWORK’S FLEXIBILITY ENABLES INNOVATION

Therefore, although the US communities shared a consensus that the current US federal privacy framework for wearables is ineffective in protecting consumer privacy, the communities emphasized the strength of the federal framework’s underregulated nature in enabling greater flexibility for businesses and, thus, more innovation. When assessing the strengths of the framework, the private sector community, in particular, often pointed to the benefit of this underregulated framework in enabling innovation, linking back to this community’s initial framing of the importance of balancing the value of innovation and privacy. Subjects in this community frequently used comparisons of companies in the underregulated wearables industry under this framework with those under the HIPAA framework. This comparison was often raised in an attempt to point out how the restrictions of HIPAA have limited the innovation in the medical device industry. One privacy researcher from the private sector community expressed this sentiment through his statement that:
…we’ve actually been able to innovate quite a bit without restrictions. The wearables industry is a relatively underregulated space…so when things are developed, no one’s asking whether this is a good idea or not or whether there might be too many harms to consumers, and therefore, we shouldn’t even consider trying to do something like this even if it does have pretty substantial benefits.

This statement suggests a common sentiment among the pro-industry communities that regulated industries often focus too much on consumer protection and overlook the substantial benefits of innovation that may outweigh the privacy risks of having less regulation in place. Many individuals from the pro-industry communities pointed to existing mechanisms in the US privacy framework that provide a balance between innovation and privacy. These mechanisms include: the opt-out mechanism available to consumers through the existing US framework’s notice and consent regime, which allows companies to offer privacy policies to individuals and these individuals have the ability to choose whether to use the technology.

4.2.3. OTHER FORMS OF OVERSIGHT FILL FEDERAL PRIVACY PROTECTION GAP

While consensus existed among the US communities regarding the US framework’s ineffectiveness in protecting consumer privacy, communities frequently raised, when evaluating the framework, the importance of other forms of privacy oversight in filling the gap in federal privacy oversight. Most subjects identified the role of US states, industry self-regulation, and the market/consumer choice as the major other forms of privacy oversight for wearables. A director of business development at a small US wearables company captured this sentiment through his statement that: “Although these forms [of oversight] protect privacy, privacy isn’t everything—people need to consider the importance of other factors too.” Yet, communities varied in their perception of the value of these other forms of privacy in filling this gap in federal privacy oversight.
In discussing the role of US states in filling this privacy oversight gap at the federal level, the US interpretive communities agreed that the oversight role of US states in implementing privacy laws is important to consider when evaluating the federal privacy framework. An analysis of interview transcripts shows that 18 of 27 individuals from the US communities mentioned the word ‘state,’ associated with the code ‘US State Oversight’, when evaluating the framework and discussing the importance of considering other forms of privacy oversight. Subjects frequently raised the US State of California as an example of a state leading privacy legislation, and many framed this sentiment with the state’s recent passing of the CCPA.

The evaluation of the value of states as another form of oversight varied across the interpretive communities. The pro-consumer protection public interest group and the US government communities associated the greatest optimism to the role of states in filling the gap in federal privacy oversight. Subjects from these communities frequently used phrases, such as “foundation of democracy” and “laboratory of democracy”, when describing the role of states as another form of privacy oversight. A policy advisor in the pro-consumer protection public interest group community suggested the importance of states in filling this gap and testing out new privacy frameworks through his statement that:

California is one of the activist states. They tend to be sort of a laboratory for experimenting with new ideas. I think there is certainly a greater sense of awareness in certain US states of the types of problems we're talking about regarding data and privacy, and some states, like California, are eager to try to find new ways to regulate to address these problems.

The private sector and pro-industry public interest group interpretive communities associated the role of the states more negatively as a form of privacy oversight. While these communities acknowledged the effectiveness of state privacy laws in protecting consumer data privacy, they stressed that other factors, including economic competitiveness and innovation, must
be considered and balanced with privacy. A senior policy advisor in the pro-industry public interest group community expressed this sentiment through his statement that:

We think that this sort of model works well, where firms are generally able to take the data and innovate...but the fact that a lot of groups and different political entities don't think that provides satisfactory protection for consumers has led to a somewhat fragmented regime in the US especially, in the data protection realm, where you have a bunch of different states passing different types of data protection laws across the country. These different state laws are beginning to come into effect and this is creating additional complexity and, at times, conflicting rules that might be difficult for firms, particularly small firms, to comply with.

Subjects from these communities emphasized that since US states can create their own privacy legislation, this has created a patchwork of privacy laws across the country that has made compliance very burdensome for companies. Subjects in these communities particularly referenced California’s 2018 CCPA to stress how state privacy oversight has the potential to inhibit innovation. This sentiment suggests the importance to these communities of considering other factors, such as innovation, in addition to consumer privacy protection, when evaluating whether other forms of privacy oversight are beneficial.

Moreover, the US communities acknowledged industry self-regulation, through implementing best practices for privacy, as another form of privacy oversight that fills the gap in privacy oversight at the federal level. An analysis of interview transcripts showed that 14 of the 27 US subjects interviewed mentioned terms related to the code for ‘Industry Self-Regulation’ when discussing other forms of privacy oversight.

The private sector, pro-industry public interest group, and US government interpretive communities associated the greatest optimism to the value of the market and industry self-regulation in filling the gap in federal privacy oversight. 13 of the 18 subjects (72.2%) from these three communities made references to the ‘Industry Self-Regulation’ code when evaluating the
existing federal framework for privacy. A former director of the FTC expressed his confidence in the role of the market in filling this gap in federal privacy oversight through his statement that:

…the market is going to change things. So, one thing that's really interesting these days is what's happened to Facebook. Facebook, in the course of a couple of years, has very much changed its business model to respond to the well-deserved criticism that it has been getting. And so, one of the things that's really interesting about this is that you see a company that has worked rather assiduously recently to radically change its business model in order to better protect privacy because its failure to do so has hurt it in the marketplace. I think one of the things that's been interesting is we've asked for a long time when are people going to push back on privacy, and I think the Cambridge Analytica incident was the catalyst. If you look at the usage rates of Facebook, they've declined pretty markedly in the last six months and most of that, I think, is attributable to the crap that it's been getting in the market, so it'll be interesting to see to what extent the market itself helps correct some of these things.

A director of an industry association for privacy experts referenced surveys conducted by his association to suggest the adoption of privacy by companies in the absence of federal regulation. Moreover, this subject used a narrative to point to the initiative taken by many major US tech companies to protect consumer privacy to highlight his confidence in the role of industry self-regulation in filling the gap in federal privacy oversight:

In the late 1990s, the first companies to appoint chief privacy officers were larger companies like IBM, Axiom, and AOL. So this is kind of tied to the Internet boom you know the tech bubble which burst sometime in 2000, but businesses at that point just realized that their future is less in manufacturing and instead in data and that data management and data governance is a strategic role and that complying with consumer expectations may be more important than purely focusing on complying with the law…and the last thing you want is to see your business practices kind of dragged on the front page of The Wall Street Journal or The New York Times business pages. So that's you know when businesses started developing privacy management programs. The market was the driver for pushing companies to adopt their own privacy policies, not privacy legislation.

The consideration of these communities of industry-self regulation as another form of privacy oversight was further in a document provided during an interview with a former privacy researcher at Intel (Intel, 2018). The document detailed Intel’s position, as of November 2018, on the US’s federal privacy framework and its recommendations for moving forward (Ibid.).
document suggests the company’s favoring of the existing limited federal oversight and its use of notice and consent to ensure privacy protection, through its proposed privacy bill to the US Congress (Ibid.). The proposed bill recommends that the US federal government maintain its current notice and consent regime, and adopt a federal framework that prevents US states from mandating their own privacy laws for companies to follow (Ibid.). This document noticeably does not suggest any additional restrictions on data use by companies (Ibid.). The bill advocates for the continued use of industry-created privacy policies to make individuals aware of any privacy risks since this mechanism ensures that companies still have sufficient data for analysis (Ibid.). Although, the company recognizes that, in most cases, people do not read the policies and are not aware of how their data is used, as is suggested in the document’s summary of the document (Ibid.):

Research shows that for the most part people do not read privacy policies. However, privacy policies can play a useful role to describe how an organization uses personal data. The law encourages organizations to create new mechanisms for individuals to provide meaningful consent for data use. Most uses of data will require a risk/benefit analysis that will restrict an organization from using data in a way that creates undue risk for individuals. However, in many situations, individuals may be ok with these risks, and will want to have the benefits of the use of the data. As artificial intelligence tools are deployed across more industry sectors, it will be critical that the data used to train those algorithms has adequate diversity and volume.

While agreeing that industry self-regulation functions as another form of privacy oversight, the pro-consumer protection public-interest community diverged from the US government and pro-industry communities by viewing this industry self-regulation negatively as a form of oversight. Conversely, to the other communities, many in this group stressed in their responses their criticism of the use of privacy policies by companies to make consumers aware of how their data is being used. Subjects in this community frequently pointed to the ineffectiveness of company privacy policies as a form of company self-regulation due to the frequency of data
practices being buried in the policies or presented in difficult to understand legal terms. A privacy policy analyst at a pro-consumer protection public interest group expressed his criticism of this form of oversight through his statement that “…it’s encouraged to tell people what your privacy practices are and be honest about it, but what those privacy practices have to be is really up to the company”. This criticism of the effectiveness of industry self-regulation as a form of oversight connects with the initial framing of this community of the importance that people understand how their data is collected and used.

4.3. PERCEPTIONS OF MOVING FORWARD

This section bases its analysis on three questions that sought to capture the symbolic words and narratives that the US interpretive communities used to convey their perceptions of how the US federal government should approach privacy for wearables moving forward. The themes that emerged in this section reflect each community’s initial framing of the value of privacy and other factors that they consider when weighing the value of privacy. To analyze how the communities assessed compare in these areas, this thesis analyzed responses to the following interview questions:

1. What is your perception of whether this existing approach to privacy should be modified to better address new technology trends like lifestyle and wellness technologies?
2. If so, why and what do you think could be done to modify this privacy approach?
3. What factors do you think should be considered in the future as the federal government considers its future approach to privacy for wearables?
4. What obstacles may prevent the potential changes that you posed from being implemented in the US?
4.3.1. IMPORTANCE OF CONTEXT AS A MOTIVATOR & OBSTACLE IN INFLUENCING RECOMMENDATIONS

Although the groups did not share similarities in their perception of how the US federal government should approach privacy for wearables moving forward, the US communities aligned in their sentiment that context served an important role in their perceptions of how the approach should be modified. 15 of the 27 US subjects interviewed framed their response to these questions with a reference to a term in the “Context-Dependent” code, suggesting the importance of recent and current events in influencing their recommendations for the future.

The communities all referred to recently-passed state privacy legislation, such as the 2018 CCPA, when explaining their reasoning for their perceptions of how the existing framework should be modified. The private sector and pro-industry public interest group communities frequently raised the recently passed 2018 CCPA when stressing their perception of the need for a federal-level privacy law that preempts state-level privacy legislation. A privacy researcher from the pro-industry public interest group community conveyed this sentiment through his explanation that: “You know the clock is ticking. People are realizing that the California Consumer Privacy Act is going to seriously impact their business—their business models and their bottom line—and they want to protect themselves against that, which is a perfectly natural instinct.” Intel’s (2018) proposed federal privacy bill document highlights state laws as a motivator for the company’s interest in federal privacy legislation:

To improve the protection of personal privacy by enacting nationwide standards governing corporations’ and nonprofits’ collection, use and sharing of personal data...A non-harmonized patchwork of state legislation will cause companies to default to restrictive requirements and the result will decrease the likelihood of realizing technology’s great potential to improve lives. Intel has drafted proposed legislation to realize that potential.
Another privacy researcher from the pro-industry public interest group further emphasized this sentiment through his focus on the importance of the CCPA not being passed due to his perception that the Act will inhibit innovation and burden US companies:

…we're seeing increasing fragmentation where you have different laws—both in the EU and California—all these different state laws coming into effect that are creating additional complexity and creating rules that might be difficult for large and small firms to comply with…So, if we could get a federal regime that can supersede, specifically the California law, but maintain the general opt-out regime, where firms are able to collect and innovate with this data without unnecessary rules that limit that collection and use, that would be good.

Similarly, the US government and pro-consumer protection public interest group communities frequently mentioned the recently passed CCPA when providing their perception that state-level privacy legislation should be pursued before a federal legislation is implemented. This sentiment paralleled their positive perspective of the role of states as a form of privacy oversight when evaluating the existing federal framework. While the US government community generally referred to CCPA and EU laws, such as GDPR, as beneficial, the group did not relate this optimism to their recommendations for the federal approach moving forward. The pro-consumer protection group referred to the CCPA as having a positive impact for consumer privacy protection. Many members of this community looked negatively on a federal legislation since state laws enable the legislation to be tested at a smaller scale. A privacy researcher at a pro-consumer protection group stated that: “We shouldn’t rush it. State legislation allows us to test laws at a smaller scale. It’s kind of cool.” These subjects frequently referred to the proliferation of the data breach law across the US, driven by states, even though the law still has not been passed at the federal-level. A senior privacy researcher at a pro-consumer protection conveyed this sentiment through his statement that:

…look at what happened with the old data breach laws. California passed it first, then it got passed by a bunch of states and that was kind of everywhere and there's no federal law
for it, but it's kind of been everywhere and if you look at history, many local laws have tended to kind of serve as templates for federal legislation because no one wants to start off from scratch at the federal level.

Yet, a few from the pro-consumer protection community viewed the CCPA as potentially negative since they fear that industry groups will continue lobbying for a weaker federal level privacy legislation to preempt the California law, as long as the CCPA is being considered. One privacy researcher from this community expressed this sentiment through her statement that: “The law isn’t even that good or worth it, to cause the loss of all the progress that California has made.”

The pro-consumer protection group further diverged from the other US communities in its emphasis on the political context of the current Trump Administration as playing an important role in its recommendation to not implement a federal privacy legislation in the near-term. When discussing how to move forward, this community frequently stated their interest in setting a higher bar for privacy in a federal privacy legislation to ensure that consumers across states are protected equally. Yet, many subjects from this community noted that they did not perceive that the current administration would prevent industry from lobbying for and having implemented federal privacy legislation that sets a low privacy compliance floor and preempts the progress made by states. Therefore, all of the members of this community referred to strengthening the FTC or banning select business data practices as modifications that should be made at the federal level. These suggestions conveyed this community’s perception that state laws would better protect consumer privacy, and therefore, the community’s valuation of consumer protection over innovation, since companies may be burdened by states implementing a patchwork of privacy legislation.

4.3.2. NOT GOING TO CHANGE ANYTIME SOON

Despite a lack of consensus across groups regarding their perception of the best course of action for the US federal government for wearables moving forward, the US communities shared
the sentiment that either nothing would change at the federal level if the California law was overturned or that the complexity of creating privacy legislation would prevent a federal privacy law from being implemented in the near future. 11 of the 27 participants in this study provided responses that fell under the ‘CCPA-Dependent’ code, and the other half fell under the ‘Too-Complex’ code. A senior policy advisor at a pro-industry public interest group expressed his belief in the importance of the California law in deciding whether Congress continues considering a federal privacy legislation through his statement that:

You have considerable support for national legislation across industry, and part of that, is the concern over states, like California, taking over and regulating this space in a way that creates you know a great deal of complexity and expenses associated with compliance costs…we will have national privacy legislation certainly before the California deadline. I think we'll see a flurry of activity you know right up against the deadlines to prevent the law from affecting their businesses.

In discussing the complexity of creating privacy law, a software developer from the private sector community conveyed his uncertainty regarding the potential of any federal privacy legislation being passed due to its potential to impact innovation and US national security:

There's also a lot of uncertainty like when it comes to technology. We're talking about a space that's moving really fast and because of that there's also this hesitation that the government doesn't want to get it wrong, in a way, you know? They wouldn't put it this way, but they don't really want to become Europe because Europe has a more passive, the kind of a slower-moving, more restricted approach to it, and you might end up with a result that has unintended consequences that handicaps the industry players. And, you want the country to stay ahead of the game. We want it to be competitive with other countries, and so I think policymakers also have to think a little bit about that and, in part, that explains the hesitancy in trying to take a more proactive or even like a paternalistic approach where you tell the industry in more specificity how they should handle it and what they can and can't do with it.

A policy analyst from a pro-industry public interest group shared a similar sentiment about his perception of the unlikelihood of the creation of a federal privacy legislation due to the difficulty of balancing innovation and privacy:
I’m skeptical that we see something happen. Folks have been talking about baseline privacy legislation for years, for like almost a decade now, and there have been a lot of conversations about a new privacy law, but none of them really make it that far…It's going to be difficult for the two parties to come together on putting actual text down. Once you get beyond sort of talking points and general support for more privacy legislation and actually try to put the pen to paper, it becomes clear that making privacy laws is not easy. You have to balance a number of competing interests: innovation--so firms being able to freely use data--and then, there are those that push for stronger consumer protections on privacy—so data collection and its use. Once you start to really try to balance those, I'm not quite as sure that the two parties will come out quite in the same place.

Yet, a few subjects from the pro-consumer protection public interest community pointed to the history of US privacy legislation to suggest that privacy laws have never been planned and that attempts at predicting the creation of new privacy laws is often fruitless since laws are frequently spurred by chance events. A senior policy researcher from this community conveyed the spontaneous nature of US privacy law through referencing the creation of the Video Privacy Protection Act:

…laws emerge from you know different motivations and some of them were reactions to just specific cases or scenarios. For example, the Video Privacy Protection Act is well-known to have been the legislator’s response to a story in the press about his record of borrowing videos—when there used to be like video rental shops—and that created a big outcry. The House and Senate rushed to pass a bill to prohibit access to this kind of data and the publication of this sort of information about an individual’s video viewing habits. So, it's kind of hard to harness the different threads of US privacy laws into one kind of comprehensive, uniform storyline.

4.4. EU ANALYSIS – INFLUENCE OF EU PERSPECTIVE

4.4.1. FRAMING OF PRIVACY

This section bases its analysis on three questions that sought to capture the symbolic words and narratives that the EU government community used to frame their definition of privacy and the meaning of privacy to individuals in this group. To analyze how the communities assessed compare in these thematic areas, this thesis analyzed responses to the following interview questions:
1. Do you think that there is any privacy risk associated with lifestyle and wellness wearable technologies?

2. Can you give me examples of what might be a risk and what might not be a risk of this technology, and what influenced your thinking about this risk?

3. What would you say are the primary characteristics of the European Commission’s approach to ensuring the privacy of the data collected by these wearable technologies?

4.1.1. SIMILAR FOCUS ON TYPE OF DATA - ALL DATA SHOULD BE PROTECTED, BUT IN PARTICULAR CERTAIN TYPES OF DATA

The EU government community shared a consensus that privacy should be ensured for all data but emphasized that certain types of data being collected should have greater privacy protection. 89% of individuals interviewed from this community used terms related to the code for ‘Type of Data,’ when framing the privacy risks of wearable technologies and for what type of data, they perceive that a user should have privacy protection for. A current European Commission data protection official informed me that when framing the value of privacy, she first determines the privacy risk of a technology and the data collected through:

…articulating what the product will do, how it might integrate different sources of data, where those data come from, who has access to them, and what happens to the composite data to add a bit of real-world utility and to think through what the implications of the technology would be.

Other subjects in this community stressed this perception that certain types of data require more privacy protection than others.

The community frequently pointed to health data as a specific type of data that posed the greatest risk to privacy. Subjects referred to health data as being particularly sensitive. A data protection official for the European Commission attributed her concern over the privacy of health data to the EU’s Article 8 (1) of the GDPR that outlines special categories of personal data that are
subject to additional protection and designates “data concerning health” as “sensitive personal
data” (OJ C 326, 26., 2012). Another EU data protection official stated that “…we consider health
data and health-related data as particularly sensitive, so having any of this data collected by these
devices...it’s already as you can see...there are quite some privacy risks posed by the technology.”

Subjects from this community often perceived aggregated data as another type of data needing greater privacy protection. My interlocutors viewed privacy protection as being most valuable for aggregated data due to the ability of this data to be used to track changes in a user’s behavior or make predictions regarding the state of a user’s health. A current academic and former EU government health official expressed her concern about this predictive capability through her statement that:

I think there are some sort of boundary issues that are really interesting when you start thinking about the interpretation of the data and how it is beginning to inform individuals actually changing their behavior or to imply that they need some sort of health intervention from health services.

A senior EU data protection official used a different metaphor to highlight the importance of privacy in protecting against the release of aggregated data:

Another risk would be something like ‘function creep’ and the capabilities that such a technology would allow organizations to be much more intrusive and collect a much higher amount of personal data. Advancing methods of assessing health in combination with new big data techniques create a privacy risk that, actually, you can read a lot more into people's lifestyles then you would otherwise have been able to do through the analysis of data.

4.4.1.2. WHO SHOULD BE SHARED THE DATA – INFORMED CONSENT BEFORE DATA IS SHARED, REGARDLESS OF RECIPIENT

When framing the risks of these technologies, the EU government community shared the sentiment that data should never be shared illegally or legally to malicious actors. Most transcripts (70%) assessed used terms that fell into the ‘No Data Sharing to Malicious Actors’ code when
discussing who should not be shared data collected by a wearable. Many study participants stressed the value of ensuring the privacy of the data from malicious actors through cybersecurity measures through the use of terminology, such as: “security of the device,” “compromised data,” “protecting against unauthorized access,” “minimizing the risk of a cyber-attack,” and “strong cybersecurity requirements.” An EU data commissioner raised the importance of an EU cybersecurity policy that the EU government is working on that will protect personal data from intrusion by malicious actors and will ensure the user is in control of information about his or herself:

You should also look at the Cybersecurity Act being worked on. This Act will strengthen cybersecurity in the EU by introducing a certification mechanism for products and services to make sure that the products on the market meet certain criteria and could be certified as cybersecured, making people have a better understanding of which products are most secure and protect their privacy.

A different EU data commissioner suggested the value of EU data protection measures in ensuring the privacy of data from malicious actors through his statement that:

I mean coming from the privacy direction. Of course, the issue of data and access to unauthorized access to data is prevalent and raises concerns with certain kinds of data. We consider health data and health-related data as particularly sensitive so having access to any amount of health-related data collected by these devices poses privacy risks.

Similarly, the EU government community aligned in their sentiment that they perceive privacy as ensuring that data is not being shared with a third party without the user’s informed consent. 63% of the interviews from this community fell into the code category ‘Shared with the User’s Informed Consent’. A senior policy analyst for the European Commission suggested the value of a user’s informed consent in ensuring an individual’s privacy through her statement:

When data is shared, sensitive health data can be stolen or used for other purposes. For example, a wearable producer could collect data for other reasons and misuse data. There is the risk that this data accumulated in one place on the health of a certain person could be stolen or used for a different purpose that originally intended. This is a risk from the side of security but also from the privacy point of view. We can imagine a situation where a wearable health company is advertising itself as a medical device, but is using the data for
other reasons like profiling and advertisements. However, now, in the EU, this misuse will be more difficult since the GDPR will limit this tracking and accumulation of information.

4.4.1.3. PRIVACY IS A FUNDAMENTAL HUMAN RIGHT

When framing the value of protecting against privacy risks posed by wearables, the EU government community shared consensus in its emphasis on the value of privacy as a result of its belief that every individual has fundamental human rights to privacy and data protection. Subjects conveyed this sentiment through 100% of those interviewed from this community using terms that fell into the ‘Privacy as a Fundamental Human Right’ code. When explaining this belief, subjects referred to World War I and World War II, in particular, as events that shaped their perception that everyone deserves privacy. An EU data protection official expressed this perception through his statement that:

In European history, after World War II, we were triggered by the experiences of World War II, where comprehensive surveillance was one of the instruments of the dictatorship regimes, which helped to commit mass-murder. So, the sensitivity here was quite strong. And, it is also enshrined—not necessarily with the same words—in many of the constitutions of European countries that controlling one’s data is necessary to preserve personal liberty and the right to develop one’s personality, which is like—which is very much like the European way of expressing the pursuit of happiness.

Another EU data protection official conveyed his perception of privacy as a fundamental human right through his statement that:

Privacy is deeply, and has been deeply, enshrined in the European way of understanding fundamental rights and human rights since the recreation of European democracy after World War II. To the disasters of the first half of the 20th century, it is basically the result of reflection and deep thinking of people who had gone through that experience and survived and wanted to find a way to avoid it occurring again in the future. In different ways, they tried to develop a system in which would have safeguards against a repetition of the events that led to the second World War and the war itself. The war had such a deeper impact on European culture than on US culture.

The EU government community expanded on this perception of privacy as a fundamental human right through its explanation that Europe has had a long-ingrained perception that this right
should be included in EU law since after World War II. Subjects made frequent references to the EU’s long-history of including a right to privacy in its legislation. An EU data protection official explained that:

There is a broad political consensus that the data processing by the state should be controlled. The first European data protection laws were adopted between 1971 and 1972 and so on. Nationwide laws in Germany and France were adopted in ‘77 and entered into force in ’78.

Similarly, other subjects in this community referred to specific policy documents further back in history that solidified in many EU member states a legal system that values privacy and believes that privacy should always be guaranteed as a right for every individual. When framing his value of privacy as a fundamental human right, a senior EU data protection officer referred to the history of valuing privacy in many European countries before the formation of the EU. He conveys this through his statement:

The Treaty on European Union, signed in 1992, which is like the Constitution for the European Union, enshrined data protection and privacy—both of them—as fundamental rights since its entry into force in 2000 in the Charter of Fundamental Rights. Data protection and privacy had already been included in the European Convention on Human Rights, which is a much older instrument with much more signatories from all EU member states and was signed in 1953…Basically, the idea of giving people control over their private life and really the early observation of controlling their own private life through giving them control about what others can do with their data.

As a result, many of the subjects framed their perception of the meaning of privacy in the EU being a natural consequence of deep reflection by individuals impacted by the World Wars.

4.4.2. EVALUATION OF EXISTING EUROPEAN COMMISSION-LEVEL PRIVACY FRAMEWORK FOR WEARABLES

This section bases its analysis on four questions that sought to capture the symbolic words and narratives that the EU government community used to convey its evaluation of the existing
European Commission-level privacy framework for wearables. This thesis analyzed responses to the following interview questions:

1. What do you consider the European Commission’s approach to ensuring the privacy of the data collected by lifestyle and wellness wearable technologies?
2. In your opinion, what do you think are the strengths and weaknesses of this approach of the European Commission to ensuring the privacy of the data collected by wearables?
3. What do you think have been the biggest influences on the European Commission’s approach to privacy and its characteristics?
4. How do you think that the EU Commission’s approach to privacy compares to that of other countries in ensuring the privacy of the data collected by wearables?

4.4.2.1. BELIEF THAT EU APPROACH REFLECTS ITS VALUE OF PRIVACY

When evaluating the EU Commission’s approach to ensuring the privacy of the data collected by wearables, the EU government community shared the belief that a strength of the current privacy framework is that it reflects the subject’s perception of the value of privacy. This evaluation builds on the EU government community’s initial framing of privacy as a fundamental human right. When responding to these questions, 100% of the subjects in this community mentioned at least one term in the ‘Approach Reflects EU Value of Privacy’ code.

The community frequently referred to the EU Commission’s privacy framework for wearables as reflecting its perception of the value of privacy. A senior EU data protection official conveyed this sentiment when he explained his evaluation of the GDPR:

The main principle seems to be, that the technology provider is responsible for the technology and the user for the use of it. The GDPR reflects that we consider data protection and privacy to be two partly different and both independent basic rights (see articles 7 and 8 in the EU Charter of Fundamental Rights).
On its website, the EU Commission defines privacy as “the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role” (European Data Protection Supervisor, 2018). EU officials interviewed frequently pointed to privacy, based on this definition, as being protected in the GDPR through its focus on principles that promote privacy protection. One senior data protection official conveyed her evaluation of the strength of the incorporation of the EU’s value of privacy into its privacy approach for wearables through her statement that:

The GDPR states that only data that is necessary can be collected unless for specific purposes; that people can correct data or delete it; and sets rules that are general enough to cover many different technologies. The GDPR sets principles such as: data minimization, which means that you collect data for specific purposes and collect data only for what you need, not more. The GDPR is trying to set the framework for general principles that have to be implemented in different technologies and that we view as being important to protect. When we have the technologies, while we are developing and working on them, it is important to translate these principles into the technologies to ensure that the technologies are compliant. Technology is changing but if you adopt general rules to follow, these will be considered when these technologies are being developed.

Another EU official conveyed a similar sentiment through her statement that: “The General Data Protection Regulation is a wholistic approach to data protection that sets out rules on how to process personal data and gives grounds for processing and lays out certain principles that the company or entity that is processing the personal data has to comply with.” Other individuals in this community shared this sentiment through referring to specific articles of the GDPR that ensure the protection of privacy. Some subjects explicitly stated their perception that the EU Commission seeks to protect privacy through its legislation. A junior data protection officer expressed this through her sentiment that:

Some may consider it [the GDPR] more traditional and strict since it includes everything in the legislation, but it is based on the EU’s belief in the rights of individuals that need to be protected and that data protection needs to have a strong, legal ground.
Two of the individuals interviewed attempted to justify their evaluation that the EU Commission’s approach to privacy adequately reflects its value of privacy protection through referring to surveys, such as Annual Track for the UK and Eurobarometer for the entire EU, which highlight that EU people value privacy. In 2015, about 50% of people in the EU stated that they were worried about the recording of everyday activities via phone or mobile applications, according to a Eurobarometer survey conducted on public opinion regarding data protection (European Commission, 2015).

Yet, most individuals in the EU government community acknowledged that EU values cannot be generalized and that divisions exist across the EU regarding the perception of the value of privacy. 67% of those interviewed from this community pointed out in their responses to these questions that EU-wide values are generalizations. A junior EU official that focuses on technology and privacy stated that: “However, some countries care less and some care more and are more vocal and seek judicial ways to make sure their rights are observed. In general, there is an increasing expectation and awareness of people for data control.” Other subjects in this community referred to specific examples that suggested their perception of each member states unique value system for privacy. Moreover, these examples were used to point out that a weakness of the EU’s approach to privacy is that the approach is a generalization of the value of privacy across EU member states. A senior EU data protection official outlined the difference in value systems between member states through his explanation that:

There are differences within the EU-the interesting point is that in the EU, data protection or privacy mean different things for different people. Like Germans for example, are very sensitive about tracking and data about them being collected and stored and accumulated and so on. On the other hand, Germans have no problem whatsoever with being obliged to carry a state issued ID card with a photo, birth date, and some other personal data with them at all times. In the UK, people have little concern about data about them being collected—much less than in Germany—but it would be an outrageous demand for them to even register at the commune of the municipality, which would be the first step in getting
a state-issued ID card. Very different views on privacy. Swedish people are also very concerned about privacy but they have nothing against everybody’s income being accessible via the tax authority website. They find it totally logical that everybody can see what their neighbor’s pay and taxes are. Yet, while there are differences, the concern for privacy is evident if you ask people: are you concerned about your privacy or are you concerned about the processing of your personal data on online services?...and these kinds of things.

Furthermore, although the EU government community conveyed a relatively optimistic evaluation of the EU’s current privacy framework for wearables, only three subjects from this community acknowledged as a current weakness of the approach its assumption that people’s values always translate into their actions, which is often referred to as the privacy paradox. Individuals frequently referred to Cambridge Analytica and genetic testing services, such as Ancestry.com, when highlighting this privacy paradox. A former EU privacy and public health official observed that:

I suppose for me one of the problems is that there seems to be a divergence between what rights are accorded to citizens in regulations such as the GDPR, and then how people actually act. I suppose a good exemplar of this is the Cambridge Analytica debacle, where obviously citizens became aware that their data has been used by Facebook for ways that they wouldn't approve of, in short. However, despite all this negative publicity that occurred around that it doesn't seem to have dented the number of users of Facebook, and it doesn't seem to have made people warier of what they disclose or really change their behavior.

Other subjects in the EU government community shared the sentiment that this privacy paradox is a weakness in the Commission’s privacy framework that will need to be addressed. A senior data protection official evaluated the issue as:

It seems to me that there's a mismatch between what the regulation provides and how people act. It seems like the expectations of citizens and users are going to be important and this mismatch between people using things like Facebook or the Ancestry testing website because they perceive that there's some utility in them, but not actually sort of translating those uses into concerns about privacy—their privacy and concerns about data security and governance. I don't know what it will take to bring those two areas of policymaking together to make them more cohesive because it seems to me at the moment that they sort of exist in parallel, but they don't really crossover with each other.
4.4.1.3. EXISTING TECH-NEUTRAL FRAMEWORK ALLOWS IT TO BETTER ADAPT TO THE EVOLUTION OF NEW TECHNOLOGIES

When evaluating the EU Commission’s current privacy framework for wearables, the EU government community frequently referred to terms in the ‘Beneficial for New Technology Adoption’ code when highlighting the strengths of the approach in making it easier for companies to abide by the EU Commission’s data protection and privacy legislation. 100% of those interviewed in this community used a term from this code, suggesting their optimism about the current approach. Under this code, subjects frequently focused on the adaptability of the framework for new technologies as a strength of the approach since the approach to privacy protection is tech-neutral. This identified strength builds on the initial framing of this community of privacy, which highlighted the belief that privacy is a fundamental human right and should be protected regardless of the technology.

When describing this strength, subjects in the EU government community often listed some of the core principles of the GDPR. For example, a senior data protection official focused on the principle of ‘data minimization’:

The GDPR is general enough to cover the evolution of new technologies. It is a set of principles that applies to all technologies—it’s technology neutral. These principles ensure that these technologies only collect as much data as is necessary, unless for specific purposes. These principles are built in. For instance, data minimization, which means that you collect data for a specific purpose and only for what you need, not more.

An EU privacy official highlighted the principles of ‘privacy by design’ and ‘privacy by default’:

The GDPR is trying to set the framework for general principles that have to be implemented in different technologies. While we are developing and working on technologies, it is important to translate these principles into the technologies to ensure that the technologies are compliant. A very important principle is privacy-by-design and by-default—the principle that when you develop something, you have these general principles in mind and build it with these in mind. We try to be technologically-neutral. Technology is changing but if you adopt general rules to follow, these will be considered when these technologies are being developed.
In addition, when evaluating the approach as beneficial for technology adoption and advancements, this community focused on its straightforward, uniform nature across all EU members states as a strength for companies manufacturing or selling in the EU and in moving the EU closer to becoming a digital single market. 65% of those interviewed in this community referred to one of the terms: ‘uniform’ or ‘straightforward,’ at least once when evaluating the Commission’s current privacy framework. A senior EU data protection officer conveyed this sentiment through his explanation that:

The EU likes to set laws that all will abide by, like the GDPR. The GDPR primarily refers to the EU’s desire for a single market and a digital single market. The EU sees the GDPR as the first step in trying to align the EU market among its members states towards one single economy and to establish universal digital protection policies.

3 of the 6 EU subjects interviewed (40%) focused on ‘startups’ as the primary benefactor of these policies. An EU policy and legal officer in the Directorate General (DG) for Internal Market, Industry, Entrepreneurship and Small and Medium Enterprises (SME) conveyed this evaluation through his statement that:

The regulations basically apply uniformly to all member states and maybe this is also to be taken into consideration when we talk about new technologies because we are particularly aware that startups, or companies in general, working on new technologies are ready to scale up and invest when they are confident that there is a legal framework to rely upon…so I think the effect of the new regulation will be a positive one. It provides more legal certainty.

The US served as a common country of comparison for the EU government community when the subjects explained their perception of the benefits of the EU’s comprehensive approach for businesses. 30% of those interviewed pointed to the US’s sectoral approach to privacy legislation as a weakness. For example, a senior data protection officer explained his belief in the strength of the EU’s comprehensive privacy framework through his statement that:
In the US, there are very specific rules on privacy and, for where there are no specific sectoral rules, there is just the occasional rulings of the courts or state law or agency enforcement practiced. The European approach is more comprehensive.

Although the EU government community evaluated the EU’s approach to privacy for wearables with optimism, most subjects agreed that future modifications will need to be made to the approach to address ambiguities and adapt to new technologies. 67% of subjects in the EU government community used terms in the ‘Future Modifications Needed’ code, suggesting the common acknowledgement in this group that, although the approach is tech-neutral and comprehensive, changes will need to be made to improve the approach. Some subjects referred to court cases as an important method to determine the modifications that need to be made in the future. For example, a former EU data protection officer conveyed this through her statement that:

The GDPR creates general principles for the processing of those data and also general principles about privacy-by-design. For example, manufacturers are required to develop systems in certain ways that enhance the privacy of data users, but I think there's lots of gray areas that are created about what data is being generated, how is it being used, how is it being transmitted, what are the controls and the governance of the data at each point...I think much more work is needed to really understand what the wider implications are.

4.4.2.2. EU REGULATORY FRAMEWORK SERVES AS A GLOBAL PRIVACY MODEL

Overall, the EU government community shared consensus in their evaluation of the strength of the Commission’s privacy framework for wearables, which they suggested through their emphasis on the approach being a global privacy model for the rest of the world. 100% of subjects in this community referred to terminology under the ‘EU Regulatory Framework Serves as a Global Privacy Model’ code, highlighting their optimism regarding the strength of the EU approach to privacy for wearables. Although many subjects recognized that the EU policies can only be compared with those of other democratic states, subjects in this community used descriptors, such as ‘world-leading’ and ‘globally-recognized,’ to convey their positive evaluation
of the EU approach as a privacy model. A senior EU data protection officer conveyed this sentiment of the superiority of the Commission’s framework as a privacy model through his statement that:

Well, I think the GDPR or the ‘European approach’, I believe is generally seen as a world-leading approach and one of the things that I think we can see is that countries that are developing privacy legislation are basing this around the approach that the European Union takes to privacy. So, I think we have the balance right in Europe, and I think that other countries in the world recognize this and see us as a leader in this area—but perhaps not all countries.

Therefore, to convey the global following of the EU approach, subjects primarily pointed to the recently modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as the ‘Council of Europe Convention No. 108 on data protection,’ which is “the first binding international instrument [that] protects the individual against abuses which may accompany the collection and processing of personal data” (Council of Europe, 1981). The modernized version of the Convention allows non-European countries to sign and ratify the Convention. Some subjects referred to specific regions and countries that have pursued the EU model and signed and ratified this Convention. For example, an EU data protection official noted that:

More countries now are following the EU model. The Convention on the Protection of Personal Data has been reformed and reviewed recently and is open for non-European countries to join. Some South American countries have done this step already and some others are contemplating it, which brings them under obligation to have at least the same principles as in the European Union (EU) data law and data protection laws, but doesn’t necessarily need to be the same procedures and instruments but to have principles, like data minimization, storage communication, purpose limitation, and lawful processing, which means consent or any other tool to keep the control, security rules, limitation of transfer and so on.

The EU government community often made note of the US’s efforts to promote its own data protection model. One senior EU policy and legal office in the DG for Internal Market, Industry, Entrepreneurship and SMEs noted that: “The US is pushing for its own model, which
basically says: until something goes wrong, you may do what you want…For the time being, this is not making much ground.” This statement referred to the US’s promotion of the 2017 Privacy Recognition for Processors (PRP) System, which offers a Trustmark certification to personal information processors (processors) in the Asia-Pacific Economic Cooperation (APEC), and the 2015 APEC Cross-Border Privacy Rules (CBPR) System for data controllers (International Trade Administration, 2018).

However, despite its optimism about the EU privacy framework as a global model, the community acknowledged that only democratic countries will be able to adopt this type of privacy framework. 66.6% of subjects in this community referred to China specifically as a non-democratic country that would be unable to adopt the EU framework. For example, a senior EU data protection officer conveyed this recognition through her statement that:

EU is setting an example for some other countries with different mentalities that seek to copy the EU model, like Japan and South Korea, that are looking into these policies to see if they are something that they want to come on board with. However, I acknowledge that countries, like China, will never follow the EU’s belief in an individual’s right to data protection because of cultural contexts and perceptions of what should and shouldn’t be protected.

In addition, in their evaluation of the Commission’s privacy framework, the community recognized that some countries may have difficulty adopting this model due to financial constraints and bureaucratic requirements. An EU policy and legal officer conveyed the financial constraints of the model through his recognition that: “I think that an obstacle to adopting the model for many countries is of course resources, which has its challenges, but what government is not threatened by budget limitations these days?” A senior data protection officer summarized some of the bureaucratic requirements that may pose constraints through his statement that:

I think that the principles of the EU policies-they are really useful and easy because they apply to all technologies. But, still, a country may have difficulty actually going the whole way in adopting the EU model because it only has these specific rules and may not have
the other necessary systems of judicial control and independent, unconditional supervision and so on.
SECTION 5: CONCLUSION

I selected this thesis topic with the intention of developing a better understanding of how well US federal legislation protects data privacy for users of new emerging technologies, specifically lifestyle and wellness wearable technologies. At a time of uncertainty in the US about the ‘effectiveness’ of the US federal government’s existing privacy framework following the occurrence of numerous devastating data breaches and the 2018 passing of comprehensive privacy legislation by both the EU and the US State of California, I sought to provide a valuable analysis of the evaluations and perceptions of US communities of the existing federal privacy framework.

I provided this analysis by adopting an interpretive policy approach and speaking to various interpretive communities in the US privacy ecosystem. These interpretive communities included: the US federal government, the private sector, and public interest groups (pro-industry and pro-consumer protection). I was not simply interested in discovering what people’s evaluations were of the current US approach to protecting privacy for wearables and how they perceived the approach should be modified moving forward. Instead, I sought to, in addition, identify what other factors influence the acceptance of these communities of this ‘inadequate’ federal privacy framework. Additionally, for comparison purposes, I interviewed European Commission officials to better understand their framing of privacy and their evaluation of the Commission’s privacy framework for wearables.

When analyzing the framing of privacy by the US communities, I, surprisingly, found that the communities shared a similar definition of privacy, and a consensus regarding what types of data can be used and shared and who can access this data without privacy being infringed upon. Moreover, I unexpectedly discovered that the US communities shared an emphasis on the importance of considering innovation as a counterfactor that needed to be weighed when
evaluating the value of privacy to them. This argument in support of innovation as a counterfactor to privacy aligns most closely with past assertions by neoclassical economists (Rubin & Lenard, 2001; 107th Cong., 2011) and industry groups (Federal Trade Commission, 1996) regarding the importance of policymakers considering the potential impact of new privacy legislation on innovation. However, the pro-consumer protection group did diverge from this initial framing of privacy by stressing that wearable users should not only be aware of how their data is utilized, but also, should provide informed consent to the collection, use, and sharing of this data. The framing of privacy presented by this group aligns with the increasingly popular definition of privacy argued by Parent (1983) that emphasizes the importance of ensuring the informed consent of the user to how their data are used and shared.

I believe that this initial framing of the importance of balancing privacy and innovation may explain my observation, regarding the shared willingness across the US communities to accept the current US privacy approach to wearables, even though they acknowledged its inadequacy in protecting consumer privacy. Similar to the findings of many prominent legal scholars (Rubinstein, 2010; Banerjee, Hemphill, & Longstreet, 2018), the thesis discovered that the US communities agreed that the US framework is inadequate in protecting privacy. Yet, these communities diverged from past legal analyses by sharing the sentiment that the framework is still beneficial, despite its underregulated nature. These communities emphasized in their evaluation of the current US framework that the framework’s underregulated nature allows more innovation to occur and has enabled other, more flexible types of privacy oversight, such as industry self-regulation, to fill this gap in federal privacy oversight.

Moreover, I found that the communities’ initial framings of how they value innovation and privacy influenced how they perceived that the US federal government should approach privacy
for wearables moving forward. Unsurprisingly, the US communities differed in how they perceived that the US federal government should proceed regarding privacy for wearables, in part as a result of these differing interpretations of the value of privacy. These differences highlight that determining how the US federal government should proceed with approaching privacy will be very difficult, as these communities have divergent interests that impact their perception of what this approach should look like moving forward.

For example, the private sector and pro-industry public interest group communities’ initial framings of privacy weighed the value of innovation as greater than the value of consumer privacy protection. As a result, these pro-industry communities shared a common sentiment that the US should pursue a federal overarching privacy framework that preempts state-level legislation and sets a lower data privacy requirement for companies. The US communities viewed the creation of federal legislation positively most likely because the legislation would protect consumer privacy, while also preempting the CCPA, which they view as burdensome for innovation.

Conversely, the pro-consumer protection public interest group community initially framed consumer privacy protection and informed consent as arguably more important than innovation. This framing arose when the community discussed its perception that the US, in the short-term, should not adopt federal privacy legislation, but instead, should continue to allow states to innovate with privacy legislation at the local level. This perception parallels the community’s focus on ensuring the most privacy for consumers, while continuing to allow innovation by companies, through the permitting of states to test out new privacy laws before they unnecessarily burden the rest of the country. Moreover, this perception builds on the community’s interest in preventing the current federal administration from implementing federal privacy legislation that the community believes would favor industry and hurt consumer protection, by preempting progress made in
privacy legislation at the state level. The US government community did not choose to comment on this matter.

However, all the communities prefaced these perceptions with their acceptance that they are largely context-dependent or context-driven, suggesting further the complexity of determining how the US federal government should proceed with approaching privacy for wearables. For example, the pro-industry communities acknowledged that if the CCPA got amended and resulted in a minimal impact on companies operating in California, then these communities would be content with keeping the current underregulated federal privacy framework. Similarly, the pro-consumer protection public interest group community stressed that privacy advocates do not believe that the current US political administration would pass a consumer-privacy focused federal legal framework and instead, would probably side with industry. The community acknowledged that if the current administration was not in power, then the group would be advocating for a federal privacy framework that sets a higher requirement for privacy protection.

Furthermore, the difficulty in determining how the US federal government should move forward was further emphasized by the communities concluding their interviews with a shared perception that, ultimately, nothing is going to change anytime soon. The primary reasons listed for this claim were the complexity of creating privacy policy that balances US values, such as: freedom of press and privacy, with US economic interests, such as innovation and maintaining free markets.

While the divide over how to move forward in the US is evident, my analysis of the European Commission’s perspective on privacy and its legal framework for privacy highlights that the US communities share a greater consensus regarding privacy than they do with other global models, such as that of the European Commission. This analysis suggests the potential for
agreement among US communities, regarding how to approach privacy for wearables, to be facilitated moving forward. This finding differs from the arguments of some legal scholars (Schwartz, 2012; Bradford, 2012; Greenleaf, 2012; Newman, 2008) that have stressed the historic role of the EU privacy model in influencing the US privacy model and Bradford (2012)’s argument that the EU’s policy decisions have influenced the rules for privacy or ‘data protection’ globally (Bradford, 2012).

While the EU perspective analyzed may only reflect the perceptions of the Commission-level community within the EU, ideologies prevail in the transcripts that highlight the uniqueness of both the EU and US privacy models. The EU government community shared an interest in allowing technology companies to succeed in the EU, but emphasized the importance of ensuring that the EU’s fundamental rights are protected. As a result, this community viewed positively the introduction of a comprehensive legislation that can be modified over time, which ensures that the EU fundamental rights to privacy and data protection are protected and provides a straightforward, but potentially more burdensome, framework for companies to follow. This model differs from the US communities’ approaches to privacy, which emphasized the importance of ensuring that innovation is protected and then, if privacy is infringed upon, legal frameworks be considered in reaction to these transgressions. The differences between the EU and US privacy models observed parallel the findings of Bellman et al. (2004) and Ybarra (2011) that these frameworks differ since they reflect differences in the cultural values and privacy preferences of individual consumers in both places.

Therefore, I conclude that determining how the US federal government should proceed with approaching privacy for wearables will be very difficult due to differing perceptions of how to move forward within the US communities. Yet, I believe that pursuing a fine balance between
the shared US values of innovation and the privacy of the consumer will be the best approach for federal policymakers. Through my analysis, I highlighted the interest of groups in strengthening the FTC’s enforcement capability by increasing its authority to impose significant and meaningful fines on companies that disregard consumer privacy. This option would encourage companies to prioritize consumer privacy and would not inhibit innovation like a formal policy could. Moreover, I propose that the US federal government create research programs that incentivize companies to design technologies that protect the privacy of wearables users, while not restricting the ability of the wearable to operate, such as through encouraging the use of privacy-preserving data mining algorithms. Such programs could model how the US Department of Energy and US Environmental Protection Agency encouraged fuel efficiency through their ENERGY STAR program, which rewards companies that increase the energy efficiency of their products with a great-for-marketing ENERGY STAR label. Instead of penalizing companies, this model would encourage wearable companies to innovate to ensure consumers that their products better protect consumer privacy.

Furthermore, the thesis revealed areas that should be emphasized in future research into the relationship between technology and privacy. Future privacy research should focus on determining those technologies that the US government could encourage companies to implement, and/or build into their products that would promote greater consumer data privacy protection. Moreover, gaps continue to exist in our understanding of which approach of the federal government to privacy would be most beneficial for smaller tech companies or startups. This perspective could provide US policymakers with a better understanding of the policies that would most benefit the startup division of the private sector, which has not been studied extensively in the literature.
### APPENDIX

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Awareness of Data Use</td>
<td>Subject refers to the importance of a technology’s user being aware of how his/her data is being utilized, when describing what privacy means to her.</td>
</tr>
<tr>
<td>Informed Consent of Data Use</td>
<td>Subject raises, when framing privacy for wearables, the concept that an individual using a technology should be fully aware of how their data is being processed by a company and consents to this data collection and use. Symbolic language used for this code includes: “right”, “choice”, and “right to be left alone.”</td>
</tr>
<tr>
<td>No Data Sharing to Malicious Actors</td>
<td>Subject expresses the sentiment that to ensure privacy, data should never be transferred illicitly, such as through a hack, or legally to malicious actors. The subject emphasizes the importance of ensuring that the technology has strong cybersecurity to ensure that the user’s privacy is not infringed upon by a malicious actor being shared the data. Symbolic language used for this code includes: “data breach laws,” “encryption,” “passwords”, “hacking”, and “stealing data.”</td>
</tr>
<tr>
<td>Shared with the User’s Informed Consent</td>
<td>Subject suggests the value for a user’s privacy of ensuring that a wearable’s user provides informed consent before a company shares his/her data to another party.</td>
</tr>
<tr>
<td>Type of Data</td>
<td>Subject makes direct/indirect or general/specific references to certain types of data as being more sensitive and having a greater need to be protected when ensuring a wearable user’s privacy. Symbolic language used for this code includes: ‘location,’ ‘heartrate,’ ‘blood pressure,’ and ‘aggregated’.”</td>
</tr>
<tr>
<td><strong>Use of Data</strong></td>
<td>Subject refers to the value of privacy for these technologies depending on how the data is going to be used. Symbolic language used for this code includes: ‘aggregation,’ ‘data analysis,’ ‘analysis,’ ‘future use,’ ‘future advancement*,’ ‘assumption,’ ‘mental state,’ ‘mental health,’ ‘insurance,’ ‘premium,’ and ‘discriminate*’.</td>
</tr>
<tr>
<td><strong>Importance of Innovation</strong></td>
<td>Subject conveys the importance of not restricting the data flows in any way unless the data is sensitive so as to not restrict innovation. Symbolic language used for this code includes: ‘innovation,’ ‘innovative,’ ‘innovate.’</td>
</tr>
<tr>
<td><strong>Inadequacy of Existing US Framework</strong></td>
<td>Subject perceives that the US’s current regulatory framework for wearables is inadequate itself in protecting privacy. Symbolic language used for this code include: “inadequate”, “the wild west”, and “not well-designed.” Narratives used to convey this sentiment focused on: the impracticality of notice and consent regime’s privacy policies with small wearables screens; the emergence of exploitative business practices; weak FTC privacy enforcement capability; and difficulty of quantifying harms for legal purposes.</td>
</tr>
<tr>
<td><strong>US State Oversight</strong></td>
<td>Subject points to the oversight role of US states in filling this privacy oversight gap at the federal level. Symbolic language used for this code includes: ‘state’, ‘NY’, ‘NY Attorney General’, ‘California’, ‘foundation of democracy’, and ‘laboratory of democracy.’</td>
</tr>
<tr>
<td><strong>Industry Self-Regulation</strong></td>
<td>Subject references industry self-regulation through implementing best practices for privacy as another form of privacy oversight that fills the gap</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Context-Dependent</td>
<td>Subject mentions context, such as recent and current events, as playing an important role in determining how the US federal government should approach privacy for wearables moving forward. An important role in these perceptions of how the approach should be modified. Symbolic language used for this code includes: ‘CCPA’ and ‘2018 California Consumer Protection Act.’</td>
</tr>
<tr>
<td>Strengthening FTC</td>
<td>Subject refers to strengthening the FTC through increasing the fees that the Commission can charge companies and the Commission’s staffing numbers.</td>
</tr>
<tr>
<td>CCPA-Dependent</td>
<td>Subject states that nothing would change at the federal level if the California Consumer Privacy Act (CCPA) was overturned.</td>
</tr>
<tr>
<td>Too-Complex</td>
<td>Subject suggests that the complexity of creating privacy legislation would prevent a federal privacy law from being implemented in the near future.</td>
</tr>
<tr>
<td>Privacy as a Fundamental Human Right</td>
<td>Subject frames a right to privacy as a fundamental human right for all humans.</td>
</tr>
<tr>
<td>Approach Reflects EU Value of Privacy</td>
<td>Subject suggests perspective that the EU’s approach to privacy for wearables reflects the EU’s fundamental right to privacy.</td>
</tr>
<tr>
<td><strong>Beneficial for New Technology Adoption</strong></td>
<td>Subject conveys their sentiment that the EU’s approach to privacy for wearables is beneficial for new technology companies and their development of new technologies. The subject uses terms, such as: ‘adaptability’, ‘flexibility’, ‘startups’, ‘uniform’, ‘comprehensive’, and ‘straightforward,’ to express this sentiment.</td>
</tr>
<tr>
<td><strong>EU Regulatory Framework Serves as a Global Privacy Model</strong></td>
<td>Subject refers to the EU’s approach to privacy as a global model. The subject uses terms such as: ‘world-leading’, ‘globally recognized’, and ‘class reference by other countries,’ to convey this sentiment.</td>
</tr>
</tbody>
</table>

Table 1. Code book developed and used for analyzing the transcripts.
<table>
<thead>
<tr>
<th>European Union</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy</strong></td>
<td><strong>Description</strong></td>
<td><strong>Privacy Protections</strong></td>
</tr>
<tr>
<td>General Data Protection Regulation (GDPR)</td>
<td>“…regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU” (European Commission, 2018)</td>
<td>1) Data Protection Impact Assessment for IoT applications; 2) Required personal data breach notification; 3) Explicit consent for lawful processing of data; 4) Privacy by design; 5) Specific regulations for the processing of personal data regarding children; 6) The right of erasure; 7) The right of access to personal data; 8) Penalties for non-compliance with GDPR; 9) Data portability; 10) Data protection officers (I-SCOOP, 2018a; I-SCOOP, 2018b)</td>
</tr>
<tr>
<td>ePrivacy Regulation</td>
<td>“legal instrument for privacy in the digital age and more specifically the confidentiality of communications and the rules regarding tracking and monitoring” (European Data Commissioner, 2018)</td>
<td>1) The confidentiality of communications; 2) Access to stored data; 3) processing of traffic and location data; 4) Notification of user of data breaches (European Data Commissioner, 2018b)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>United States of America</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy</strong></td>
<td><strong>Description</strong></td>
<td><strong>Privacy Protections</strong></td>
</tr>
<tr>
<td>Section 5(a) of the Federal Trade Commission (FTC) Act</td>
<td>The basic consumer protection statute enforced by the FTC</td>
<td>&quot;unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful” (Federal Trade Commission, 2008)</td>
</tr>
</tbody>
</table>

Table 2. EU Commission-Level and US Federal-Level Privacy Frameworks for Wearables
Framing Privacy

1. Do you think that there is any privacy risk associated with lifestyle and wellness wearable technologies?
2. Can you give me examples of what might be a risk and what might not be a risk of this technology? What influenced your thinking about this risk?
3. What would you say are the primary characteristics of this US approach to ensuring the privacy of the data collected by these wearable technologies?

Evaluation of Existing US Federal Privacy Framework for Wearables

1. What do you consider the US’s approach to ensuring the privacy of the data collected by lifestyle and wellness wearable technologies?
2. In your opinion, what do you think are the strengths and weaknesses of this approach of the federal government to ensuring the privacy of the data collected by this technology?
3. What do you think have been the biggest influences on this US approach to privacy and its characteristics?
4. How do you think that the US’s approach to privacy compares to that of other countries in ensuring the privacy of the data collected by wearables?

Perceptions of Moving Forward

1. What is your perception of whether this existing approach to privacy should be modified to better address new technology trends, like lifestyle and wellness technologies?
2. If so, why and what do you think could be done to modify this privacy approach?
3. What factors do you think should be considered in the future as the federal government considers its future approach to privacy for new technologies?
4. What obstacles may prevent the potential changes that you posed from being implemented in the US?

Table 3. Interview questions for individuals from the US community.

Table 4. Interview questions for individuals from the US community.
BIBLIOGRAPHY


15 U.S.C. § 45(a) (Section 5 of the FTC Act)


Brill, J. “Millions use Microsoft’s GDPR privacy tools to control their data — including 2 million Americans.” (2018).


Charara, S. “Your fitness app's privacy policy may be about to change – and that's a good thing.” (2018).


De Montjoie, Yves-Alexandre, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel.


I-SCOOP. “General Data Protection Regulation: the online guide to the EU GDPR”. (2018b).


Sepulveda, D. “What the global Internet’s stakeholders can learn from Europe's new data law.” (2018).


Yanow, Dvora. "Organizational ethnography and methodological angst: myths and challenges in
