Re-Thinking Privacy for the Physical and Digital World: Reformulating Our Theoretical Foundations

Dwight Hunter
Department of Informatics and Media
Media and Communication Studies
Uppsala University
2014

Advisor: Magdalena Kania Lundholm
Abstract

When scholars address privacy as a condition in contemporary society it can become a very difficult subject to approach on a general level. With public concerns rising surrounding matters of digital tracking and surveillance discussions of privacy have found a new dimension in digital information. Yet defining how digital privacy should be approached, in particular regard to a general conception of privacy, remains unclear. Research spanning across the social sciences, law, economics and technical fields have all taken their own perspectives towards studying various forms of privacy. This study seeks to unify privacy-related discourses by evaluating the conceptualization of privacy throughout existing literature in order to determine what fundamentally distinguishes digital privacy from general privacy while remaining intrinsically related. To do this, I employ Michael E. Brown's 'sub-theoretical notion' (2014) to turn privacy discourses inwards, seeking the underlying logic contained within its seemingly disparate dimensions. Using a sample of 28 purposively selected texts analyzed through a structural content analysis, resulting in a refined sample of n=4,486 structural elements contained within the texts, the various relational dynamics of privacy discussions are evaluated noting their interrelations. I arrive at information tangibility and loci of control as the two most intrinsic elements of privacy, dramatized by developments in technological mediation, which can thus both unify and distinguish the various forms of privacy research. In a discussion of implications of this exploratory study, I conclude with how the integration of privacy's sub-theoretical notion (information tangibility and loci of control) allows for current privacy-related discourses to acknowledge not only their own limitations to social life, but to move beyond the singular notion of a correct conception of privacy to see instead how each conception is interrelated via the unifying logic of the sub-theoretical.

KEYWORDS: privacy, e-commerce, commodification, multidisciplinary, sub-theoretical, advertising, information society, structural content analysis, internet
Table of Contents

Abstract ............................................................................................................................................... 2
Acknowledgements ............................................................................................................................ 5

PART I: Overview of the Study
Chapter 1- Introduction .................................................................................................................... 7
Chapter 2- Background ...................................................................................................................... 10
Chapter 3- Literature Review ............................................................................................................. 13
  3.1 “Free Content” Isn't 'Free' ........................................................................................................... 14
  3.2 Privacy and the Policies that Regulate It ..................................................................................... 16
  3.3 Privacy Policies as a Source of Potential Privacy Harms .............................................................. 17
  3.4 The Struggle of Research ............................................................................................................ 21
    3.4.1 The Problem of Putting the “Digital” into Privacy ................................................................. 21
    3.4.2 The Need to Move Beyond Economics ............................................................................... 22
  3.5 Concerning Media & Communication Studies ............................................................................ 24
Chapter 4- Research Problem & Questions ......................................................................................... 26

PART II: The Structural Content Analysis
Chapter 5- Methodology .................................................................................................................... 27
  5.1 Analytical Method ....................................................................................................................... 27
    5.1.1 The Sub-theoretical Framework ............................................................................................ 27
    5.1.2 Using Structural Content Analysis ....................................................................................... 33
  5.2 The Sample .................................................................................................................................. 35
  5.3 Description of Selected Texts ...................................................................................................... 37
    5.4.1 Represented Domains .......................................................................................................... 37
      Graph 5.1- Representation of Primary Disciplines in Sample ..................................................... 37
      Graph 5.2- Simplified Distribution of Primary Disciplines in Sample ........................................ 38
    5.4.2 Represented Genres .............................................................................................................. 39
      Graph 5.3- Genres of Selected Texts ............................................................................................ 39
    5.4.3 Determining Representation ................................................................................................. 39
    5.4 Establishing Validity & Reliability for the Study ..................................................................... 40

Chapter 6- Preparing the SCA ........................................................................................................... 42
  6.1 First Iteration ............................................................................................................................... 42
    Figure 6.1- Sample of Structural Outline Format ......................................................................... 44
    Figure 6.2- Use of Notes ............................................................................................................... 45
  6.2 Second & Third Stage Iterations ................................................................................................ 46
    Figure 6.3- Structural Element Reductions in Data ...................................................................... 47
  6.3 Coding to Uncover Levels of Abstraction .................................................................................. 48
    Figure 6.4- Complexity of Structural Element Relations when Coding ...................................... 49
    Figure 6.5- The Higher Elements of Privacy's Sub-Theoretical Notion ........................................ 51
    Figure 6.6- The Lower Elements of Privacy's Sub-Theoretical Notion ........................................ 51
    Figure 6.7- Identified Fields .......................................................................................................... 52
    Figure 6.8- Subject Levels ............................................................................................................. 52

Chapter 7- The Structural Elements Themselves As Things Stand ................................................... 54
  7.1 Structuring the Structural Content Analysis ............................................................................. 54
  7.2 The Umbrella that is Privacy ..................................................................................................... 56
7.3 Sub-Classes of Privacy ................................................................. 58
  7.2.1 Communication Privacy .......................................................... 59
  7.2.2 Locational & Mobile Privacy ......................................................... 59
  7.2.3 Medical Privacy ........................................................................ 60
  7.2.4 Children's Privacy ..................................................................... 60
7.3 Major Conceptions of Privacy ......................................................... 61
  7.3.1 Privacy as Control ...................................................................... 61
  7.3.2 Privacy as a State ...................................................................... 63
  7.3.3 Privacy as a Right ...................................................................... 64
    7.3.3.1 Using Laws to Impose Privacy Rights ...................................... 66
    7.3.3.2 Privacy Under the Laws of Property ....................................... 68
  7.3.4 Privacy as a Commodity .............................................................. 70
    7.3.4.1 Economic Properties of Information: Marxist Perspective ........ 71
    7.3.4.2 Privacy with the Values of Property ........................................ 72
    7.3.4.3 Impact of Data-Based Subscriptions ........................................ 73
      Table 7.1- Types of E-commerce .................................................... 75
    7.3.4.4 Contracting Privacy in the Lens of Autonomy ......................... 75
    7.3.4.5 Beneath the Veil of E-Commerce .......................................... 76
    7.3.4.6 Privacy Concerns ................................................................... 80
    7.3.4.7 Commodity Based Theories .................................................. 81
    7.3.4.8 Summary .............................................................................. 83
  7.3.5 Contextually Bound Privacy ....................................................... 84
  7.3.6 Privacy as Boundaries ............................................................... 86
7.4 Contested Signifiers of Privacy ....................................................... 89
  7.4.1 Architecture ............................................................................. 89
  7.4.2 Anonymity .............................................................................. 90
  7.4.3 Security ................................................................................... 91
  7.4.4 Surveillance/Dataveillance .......................................................... 93

PART III: Results, Discussion and Conclusion

Chapter 8- Results of the Structural Content Analysis ....................... 96
  8.1 The Dialectic for Producing Privacy's Sub-Theoretical Notion .......... 96
    8.1.1 Finding a Pattern Across Privacy's Conceptualizations ............... 96
    8.1.2 The Higher Elements of Privacy as a Sub-Theoretical Notion ....... 100
    8.1.3 The Lower Elements of Privacy as a Sub-Theoretical Notion ....... 102
Chapter 9- Discussion ......................................................................... 105
  9.1 The Significance of the Findings for the Human Sciences ................. 105
  9.2 The Significance of the Findings for Media and Communication Studies 106
  9.3 Reflection on Methodologies ....................................................... 106
Chapter 10- Conclusions and Implications for Future Research .................. 108
  10.1 Privacy as a Sub-Theoretical Notion: The New 'As Things Stand' .... 108
  10.2 Implications for Future Research ................................................ 109
  10.3 A New Personal Agenda for Privacy Research ................................ 110

References ....................................................................................... 111
APPENDIX A ................................................................................ 119
APPENDIX B ................................................................................ 121
Acknowledgements

The satisfaction I find in the completion of this thesis comes only because of the people I drew support from:

To Michael W. Raphael. An invaluable colleague and, most importantly, a great friend. With five years of academic discussions providing a wealth of inspiration and cooperation, without your help I would never have been able to wade through the complexities of this project. Your support brought about the clarity and confidence necessary to complete this. I owe you a great debt of gratitude.

To Joel Purra. Your insights into privacy from a technical perspective were instrumental in overcoming my own technical limitations. I sincerely hope that the benefits of our meetings were mutual and that we can help inspire future computer science/social science collaborations.

To Alexandra Holm. Thank you for staying with me throughout this long and difficult process. Through sleepless nights and never-ending hours, countless inconveniences and emotional struggles you kept me going. You gave me reprieve and comfort. I do not know how I would have managed without you.

To all of my Swedish friends. Thank you for the great company and adventures over the years. A good Swedish fika shall forever be a cherished part of my life.

To Gästrike-Hälsinge Nation- It was an honor and great pleasure to have worked with so many of you. Without you guys I probably would have graduated on time.
PART I: Overview of the Study
Chapter 1- Introduction

What is privacy? This seemingly straightforward question has no simple answer. Consider for a moment what privacy means in contemporary society. We can define moments, objects, feelings and spaces all as “private”. We would be hard pressed to imagine a functional society without any conception of privacy. So, despite being an intricate part of our everyday lives, defining what privacy is, regardless of context, becomes no simple task. Due to its inherent ambiguity as a descriptor, privacy remains an enigma in scientific research. This is not to say that academia has not attempted to provide a singular definition of privacy. Historically privacy had been rooted solely in the physical domain where it was commonly restricted to matters of personal belongings and spaces. In their 1890 seminal article, Samuel Warren and Louis Brandeis famously defined privacy as a “right to be let alone” (1890, 1); an elegant attempt to capture the essence of privacy as an individual's right to express dominion over certain aspects of their life, this definition continues to be utilized by researchers to this day. However, in contemporary societies privacy has found new dimensions via the qualities of digital information. In a time where social media and global information networks reign supreme, the idea of having a “right to be let alone” no longer applies as seamlessly as it once did. Armed with cellphones, laptops and an ever increasing degree of connected devices fed by a growing desire to broadcast our lives- what does it really mean to be “alone”?

Privacy is no longer a concern exclusive to the physical realm and, as such, the very conditions of privacy have shifted. Taken as a social phenomenon, our conception of privacy is being fundamentally altered by our current historical and cultural situation. In effect, it appears that existing technological developments have exaggerated any previous forms of privacy to the extent that it can no longer be subject to the same form of law, economy and polity once considered sufficient. Therefore we find the interpretations and accuracy of any one definition of privacy continuing to circle around in academic debate.

Herein rises the what is perhaps the most baffling of dilemmas for those seeking to understand the modern conditions of privacy: questioning what privacy actually is no longer serves as the driving source for academic discovery. Instead, the predominate theme of research has become the classification and operationalization of various types of privacy (e.g., digital privacy and physical privacy) justified only within their particular applications. Rather than seeking to identify what privacy is as a whole, “privacy”, as an academic concept and phenomenon, has been reduced to the discussion of specific situations/contexts. While
this approach relieves the burden of discovering what a greater definition of privacy would be, by limiting privacy into a more manageable form for study, it has also erected barriers, isolating privacy studies into incongruent segments. One can study situations of digital privacy, physical privacy or a blurred line of transcendence towards general privacy without having to demonstrate greater concern for how each segment fits together. This presents a fundamental theoretical issue for privacy-related research: how can research from seemingly distinct instances of privacy, studied under different conceptions, be related?

Existing research faces confusion over the matter of distinguishment and if/when a definition of “privacy” must apply to various contexts. At times researchers still subsume digital privacy under a more generalized conception resulting in, what can still be seen as, problematic applications of general privacy concepts (e.g. “the right to be let alone”) without regard for the arising implications. Meanwhile, researchers moving in the opposite direction have taken steps to produce nomological models of privacy specific only to digital contexts (Smith et al. 2011, 990). However, this process leaves out the very question of why an understanding of general privacy has become inexplicable and, in consequence, what theoretically justifies both types as matters of the same social phenomenon (privacy) despite remaining unique. Academia is left with a wealth of accumulating privacy-related knowledge but a diminished capacity to relate findings without a way to transcend the limitations caused by privacy's numerous forms.

This study seeks to explicate how privacy, as a social phenomenon, has been fundamentally altered by the course of technological evolution, resulting in the seemingly independent conception of digital privacy, yet can still be theoretically grounded in general privacy. In this manner, I seek to take the first steps towards resolving the struggle scholars have encountered in finding an agreeable conception of digital privacy which, only by being theoretically grounded, can still be understood as unique form of general privacy. This process is motivated by a set of basic questions: (1) how did we arrive from privacy rooted in the physical world to the digital; (2) what has changed in our perception of matters of privacy; and, ultimately, (3) has privacy itself changed as a social phenomenon? To answer these questions, I seek the common and intrinsic qualities of privacy, derived from a critical analysis its various conceptions and their related elements, as reflected in the current state of privacy research.

My approach employs the analysis of 28 purposively selected books on the topic of
privacy. By taking this dataset as representative of how things stand in regard to the various conceptions of privacy, I employ Micheal E. Brown's *sub-theoretical notion* (2014) to study the “life of the concept” in respect to privacy's continuous conceptual refinement over the course of academic and technological development. By uncovering the sub-theoretical notion of privacy it then becomes possible to reveal the initial intrinsic conditions of privacy, as a social phenomenon, which gave rise to the need for its refinement in studies. This process re-establishes what are the foundational, irrepressible, qualities of privacy carried implicitly across all of its conceptual developments regardless of context, academic domain or approach. In order to find the sub-theoretical notion of privacy, my study has been organized via the exploratory use of a structural content analysis; an emergent methodology which allows a researcher to efficiently organize a large quantity of information by focusing exclusively on drawing out the relationships between theoretical objects and their related signifiers rather than the details of an argument.

Upon completing this process, I find the sub-theoretical notion of general privacy and, by extension, digital privacy to be the interrelation between that of information tangibility and that of the loci of control. Through this lens one can then realize that academic discourse, by seeking to only study situations of privacy, has become limited because due to its fixation upon how people act instead of how they live. Discussing the implications of this discovery, I conclude that the application of privacy's sub-theoretical notion (information tangibility and loci of control) to existing/future studies can allow privacy-related discourses to acknowledge not only their own limitations to social life, but to move discourses beyond the singular notion of a correct conception of privacy to see *instead* how each conception is interrelated via the unifying logic of the sub-theoretical.
Chapter 2- Background

A need for the theoretical unification of privacy research is a direct result of its complexities which have thus far only obfuscated what privacy actually is rather than illuminate it. For the unfamiliar researcher, these complexities may not be apparent at first. However, by briefly reviewing the many forms of privacy and ways various fields approach this phenomena it becomes possible for one to become, if not well acquainted, at very least, aware of how complex the matter at hand is.

Privacy, for the purposes of this study, is to be considered, at its core, a social phenomena. The reasoning for this relates back to the very first sentences of the introduction: try to imagine a society without privacy. To call something “private” conjures images of isolation or the exclusion of others. Privacy can be a feeling– when holding a discussion in a public space it is commonly considered to be “private” amongst those involved. A potential eavesdropper would be shunned for attempting to ascertain information they have not been directly privy to. Privacy can describe a state of being or condition– one often considers the confines of their own dwelling to be a “private” space free from the intrusion of others without invitation. An action can be considered private such as going to the bathroom. Yet, privacy can also be used describe a quality, such as in the case of declaring a object to be “private property”.

By taking into consideration the statements above, privacy is found to be both individually subjective and socially molded. What I consider to be a private situation might be different from what you consider private. Meanwhile, both of us can have different expectations of privacy compared to someone of another culture. The many different attitudes held globally around issues of public nudity and sexuality are of the most easily recognizable examples. However, regardless of individual views, what any instance of privacy involves is the presence or absence of others. The concept of privacy would be rendered meaningless in total isolation from others because, in the most ironic of ways, to have privacy requires the presence of others, even if it is merely for the sake of acknowledging their absence. This simple fact demonstrates the inherent social root of privacy.

Yet, privacy itself is not a subject exclusive to the domain of the social sciences. Up until now the mentioned examples have been, quite deliberately, kept to the physical domain. This is for good reason, once the digital has been brought to the table, specifically digital
information, the entire concept of privacy becomes far more complex. Data, as an electronic form of information, composes any action online or information placed online. This means that data can be linked to physical information and existing knowledge. Furthermore, through servers and information networks, data can be aggregated and analyzed by automated processes with increasing ease. Therefore we encounter the fundamental issue that one cannot truly be “alone” online in the metaphorical equivalent of physical isolation. Any action online, by the very definition of being online, can be or is recorded, albeit explicitly or implicitly.

Although I may be alone in a private room using a computer, utilizing a search engine to browse various websites and checking my email, I would be wrong to assume my actions are private. My email server is actively scanning what I type and read. The search engine I use is storing my search terms and recording what I click. Then, to make matters even more complicated, all of this information and more is being silently gathered by cookies and other trackers, installed on each webpage I visit and used by the services themselves and other affiliates, to then be accumulated into profiles creating ever more enticing marketing profiles which can sold and/or utilized in countless ways. Add to this the thought of posting a “tweet” on my Twitter account, along with a picture, which is shared simultaneously across all of my social media profiles through an app on my phone. Without knowledge of my application's settings it has also used my phone's internal GPS to mark where I am. All of this information is being transmitted through and sent out to an audience which is increasingly difficult to identify not just on personal but also a technical scale. When I am online I am in a room full of familiar and strange faces with very little capacity to fully understand who/what might be watching. Nor can I be certain that I wont be confronted about something I’ve done/shared by someone I didn't even realize could know anything about me. Suddenly, the social nature of privacy begins to bear an obvious, intrinsic, relationship with not just the social sciences but the technical, legal and economic domains.

Although each of these fields may address the issue of privacy, quite possibly the very same situation/topic, but each can vary by approach and/or an emphasis or lack of emphasis on what other fields have to say. Privacy, from an economic perspective, is primarily related to the behaviors of individuals as consumers. Legal fields question if and how privacy should be protected by governments through the enforcement of laws and judgement of contracts. This in contrast to the social sciences which seek to understand privacy as a behavior
inherently rooted as a malleable condition of an individual within society. Meanwhile, more specific to digital conceptions, technical fields must question the pragmatic realities of privacy mechanics within digital infrastructures, often placing a heavy degree of emphasis on security via programming and encryption. However, none of these general perspectives are necessarily mutually exclusive when discussing privacy. Instead, they represent a complex web of multiple rationales capable of borrowing and/or subsuming various elements and/or arguments of any other disciplines.

Although this multiplicity is exactly what composes the richness of privacy knowledge, there is an inherent struggle to discern how all this knowledge fits together. While each field's unique perspective and focus of study is valuable in this regard, they are also incomplete and commonly flawed on a theoretical level. This is because they fail to facilitate cross-disciplinary coordination nor the acknowledgement of what privacy is at a grander scale. It is in this manner that we arrived at the current conundrum of privacy research. Any specific conception of privacy or exploration of a privacy-related topic tends to overlap and/or place different emphases, dependent upon the native perspective established by a researcher’s specific domain. Links can be drawn and different research cited from within and outside of a native field but broader context is left out. At this point in academic progression there is no clear way to actualize the ways privacy itself, as an academic concept, has been altered across studies thus enabling research to transcend the ambiguity of privacy as a whole, beyond merely relating those specific elements which hold a direct relation. The goal of this study, in developing the sub-theoretical notion of privacy, will provide this exact link between privacy studies across all involved academic domains. It acts as a bridge between digital and physical privacy conceptions by establishing the fundamental theoretical qualities of privacy as a social phenomenon on a generalized level. In this capacity, finding the sub-theoretical notion of privacy redirects the individual links between privacy-related topics and its conceptions, existing only within the study itself, and provides a theoretical foundation through which any privacy-related study can be analyzed as an emergent form of privacy beyond its enigmatic state.
Chapter 3- Literature Review

Given the ambiguity of privacy, the multitude of its conceptualizations and the sheer scope of topics/approaches possible a traditional literature review is not feasible. There is no straight-forward manner in which one can immediately produce an approachable method of summarizing the entirety of privacy research in a reasonably condensed format. Rather, the very act of finding a means to discuss the involved literature in a suitable capacity becomes the very product of its analysis through the structural content analysis (SCA) discussed later on. Therefore, it becomes necessary to refrain from an in-depth review of privacy until the SCA provides the logical structuring required to present a coherent “life” of privacy as a concept rather than a repetitive summary of disjointed discourses with superfluous argumentation. To move forward without the aid of the SCA would present a flurry of privacy-related knowledge which could only reflect the existing disjointed nature of privacy research and struggle to provide a reader with anything more than basic facts at face-value. What I offer in its stead is an introduction as to how and why privacy has become subdivided into its primary categorizations: general, digital and physical. While the goals of this study are to theoretically unify these conceptualizations, this process relies upon an understanding the how we arrived at our current distinctions. Providing this establishes knowledge which will later be utilized in seeing how digital privacy is unique while, simultaneously, inherently related to general privacy and, by extension, physical privacy.

In Chapter 2, I cited various examples to demonstrate which academic domains are inherently involved with privacy-oriented research. The most fundamental of these relationships was that between the social sciences and law. Both of these domains are easily associated with privacy, with one such example beginning at the physical level with “private property”. Systems of governance enter into a functional relationship with society by enforcing specific social norms and values, such as those revolving around the concept of privacy, through law. However, as the discussion moved into the digital realm the more direct involvement of the economic and technical domains became apparent. It is this shift in emphasis which will become tantamount for understanding the unique essence of digital privacy and, in what seems to then become a necessitated dichotomy, the opposite distinction of physical privacy.

As a consequence of the seemingly dichotomous relationship between physical and
digital privacies, the exact role of general privacy becomes lost. As we shall see later on, although it is not unique from digital or physical forms of privacy, a reference to general privacy lacks the theoretical clarity necessary to elicit any exact relationship with its counterparts. We find the phrase “general privacy” existing as a container for rather than a bridge between other forms of privacy. There are links between all three but no clear definitions to describe their relationships.

However, to a certain extent, it is only thanks to this predicament that it has become possible grasp what the theoretical foundations of privacy are as the bridge between the distinctions of physical and digital privacy. By studying digital and physical privacy as unique conceptualizations academia has inadvertently produced a juxtaposition which allows for a common theoretical ground to be discovered via their commonalities and differences. Although what has not changed over privacy's development as a concept will later become the focus of this study this only becomes possible by first realizing what is new to the conditions of privacy. To do so, I start with looking at what defines privacy's latest embodiment in the form of digital privacy. How has it come about? What is unique to situations of online privacy? Which academic rationales are utilized? In this capacity digital privacy becomes the initial point of study despite being the youngest and most complex form.

3.1 “Free Content” Isn't 'Free'

To understand the conditions which have brought about the majority of digital privacy research, one needs only to look at the very act of being online. The saying “if you're not paying for the product, you are the product”, along with its many variants, has found a certain resonance online. Although this ambiguous declaration makes a rather dichotomous claim, it holds an underlying truth. Traditional commerce, as the exchange of currency for a good/service, is no longer the primary model for electronic commerce. Since the innovation of Web 2.0, there has been an on-going shift in the nature of commerce away from traditional transactions towards what can be best described as data-based subscription services (Raphael 2013). This same shift can be considered the later iterations of what was first described as the “post-industrial” society by Daniel Bell (1973) and later as an on-going restructuring of society towards informational capitalism as defined by its techno-economic system in Manuel Castells' trilogy *The Information Age* (2010).

The prevalence and rapid development of electronic commerce, particularly that of
free-content services, is a re-enforcing and self-perpetuating crisis of information production and commodification. While traditional forms of buying and selling goods will undoubtedly remain, it no longer exists as the solely dominant form of e-commerce. In data-based subscription services the service is ad-supported and include many major companies such as Google, Facebook, Twitter, and Yahoo. The end user becomes a source of valuable and marketable information, otherwise unavailable to those the user is not in contract with. As a result, the contractor (i.e. website/service) is able to create an economic model of “free content” where the user's information is the source of value beyond their costs of operation (Raphael 2013a).

This shift in dominant internet commerce also constitutes a shift in the relation between servicer and user which impacts the public's understanding of privacy. Value generated from user-data is aggregate and potentially limitless, surpassing the value of what the “free service” provides in exchange. For the end users of these services, however, it is not necessarily clear how their online actions and communications constitute a form of commercial activity. Despite this fact, due to the continued success of the data-based subscription service model, the conditions of e-commerce are continually developing in a direction which relies upon the commodification of user-generated data for revenue.

Therefore we arrive at the impasse of contemporary privacy concerns: the ease at which technological developments have allowed personal information to be gathered innocuously from online users to create detailed reflections of our lives with a troubling degree of accuracy, for the purposes of capital production, presents the real-world problem of conceptualizing privacy in a functional manner while ensuring both public satisfaction over privacy standards and continued success of information-based economics. In this capacity, it is clear how modern economics have begun to generate concerns over individual privacy. Privacy is now subject to a dominant economic model which seeks to derive profits from personal data. However this model is unique to digital activity, separating it from the conditions of physical privacy. Understanding the impacts resulting from how data-based subscription services function not only establishes its importance for a conception of digital privacy but also establishes how complex the intertwining relationships between e-commerce and privacy are.
3.2 Privacy and the Policies that Regulate It

“I don't know what they want from us anymore. Don't they realize we agree with them?” - Eddie Izzard, Comedian

“I agree” may be the most misunderstood and misrepresented declaration of modern times. With nearly every website, application or digital service visited/used, a person “agrees” to some form of terms and conditions. Explicitly forming this agreement is often as simple as clicking a box. However, in a more troubling sense, even the mere use of website can implicitly constitute consent and this model is something relatively new to society on a general scale. There was no agreement or contract to sign before calling someone on a public phone, picking up a newspaper, or watching public television. But when using a smartphone, reading a news article online or watching videos on YouTube, there is. The question stands, what is being agreed to?

Online terms and conditions are usually located somewhere on the webpage labeled as Terms of Service (TOS) or Terms of Use (TOU) and accompanied by a Privacy Policy (PP). Combined, these two articles layout the rules that users of a service agree to. These delineate not just the rules limiting user conduct but also the service's own self-imposed rules about how a user will be treated by the service itself. Of particular note, a privacy policy will describe what types of data are collected and how data will be utilized. Through the mere presence of these documents and the continued use of a service, users can thus have legally declared “I agree” without even clicking a box.

A failure to adequately understand consent or the policies themselves while utilizing online services presents one of the major areas of study in digital privacy. Roughly 2.8 billion people, over a third of the world's population, currently have access to the internet (Internetworldstats.com, 2013) and are thus subject to the terms and conditions of any services visited. Therefore we find that specific digital media giants have come to represent facets of everyday life for the connected individual. For example, Facebook alone has reported 1.32 billion monthly active users (Facebook Inc., 2014) which constitutes nearly half of the globally connected population. Inclusion, via the use of these services, requires non-negotiable consent meanwhile exclusion can represent a disjuncture from everyday interaction. For many people, withdrawing from one of Google's 70 services (including their search engine, G-mail and YouTube), Facebook or Twitter is a crippling thought. Yet, it is
safe to assume that just these three organizations combined subjugate well over Facebook's 1.32 billion individual users world-wide to their digital policies. In effect, a modern form of a Faustian bargain is formed on a global scale (Raphael 2013a). Those who do not use particular platforms can face potential communicative disadvantages and/or the loss of private or professional contacts and opportunities as opposed to those who consent to unilateral terms and conditions (Fuchs 2011). In this sense, one can get the impression that major companies such as Apple, Google, Facebook, LinkedIn or Twitter are key protagonists when it comes to discussing standard-setting for personal data treatment (Hornung 2013).

The economic component of privacy and, by extension, everyday life becomes a forefront matter in the digital world. Under the terms and conditions of use that end-users agree to, online interactions are repurposed, to some degree, for profit-generation by the service. However, both the agreement and the literal transaction are consistently hidden outside of what is stated in the terms and conditions, even if read by the user. In effect, the context of digital-interactions have moved beyond the initial intentions/understanding of the user. Their awareness of this shift is paramount to their ability to understand how generated information can be and is repurposed since, for access to services, users must agree to a deal which permits the access, gathering and use of their information.

Digital privacy researchers thus find themselves fixated on determining if the public has sufficient knowledge of the terms and conditions users face online to understand the sources of potential privacy harms. Scientifically measuring user rationality/autonomy becomes essential for an explanation of privacy in this regard. Although this argument could have been formulated on general terms, in an effort to further distinguish digital privacy as unique, current research contrasts the diminished capacity of individuals to act in a rational manner online versus in the physical world. While this has its merits in accumulating knowledge about specific privacy situations (elaborated below in Section 3.3), it also inadvertently constructs a perceived delineation between general and digital privacy as completely separate phenomenon precisely because of how established rationales related to the physical world fail to apply online.

3.3 Privacy Policies as a Source of Potential Privacy Harms
Rationality becomes a means for scientists to measure an expectation of privacy in contrast to reality. If users of online services are acting in a “rational manner” then that logic of
rationality would presume they have made an informed choice by accepting a set of terms and conditions with the understanding of how their personal data will be utilized. Sound in theory, a privacy harm thus arises when end-users experience a use of their data by a party who violates their understanding the agreement. This places the burden of a privacy harm on the terms and conditions itself. When users seek recourse for a privacy harm, the economic model of data-based subscription services then relies upon a legal interpretation of their actions to be not only within the scope of their agreement with end-users but also within their greater legal capacity as a market regulated by law. Digital privacy then brings forth a secondary relationship with the legal domain, which had previously only been regarded as an enforcer of privacy, where the economic value of diminished privacy standards exists in contest with the social desires/expectations of end-users. The role of law becomes pivotal on both fronts and specific cases in recent history can demonstrate how obfuscated and complex these relationships become.

In a document released by Edward Snowden, it was revealed that the National Security Agency's (NSA) PRISM program, engineered for broad-scale surveillance, aggregated data from providers such as Microsoft, Google, Yahoo!, Facebook, YouTube, AOL, Apple and others, thus covering most forms of digital communication (Washington Post, 2013). The actions of the NSA, although viewed as legal within the greater regulatory framework of the United States government, became one of the most far reaching examples of what can happen when a disjuncture of rationales surrounding the legal protections of privacy occur amongst not only US citizens but also for global audiences utilizing these services. As diplomatic fallout continues, primarily stemming from international disapproval over the United States' legal frameworks treatment of privacy, it has lead to the European Parliament passing regulations to prevent the transfer of data to US corporations in addition to US based members of the telecom industry loosing international contracts due to rising concerns over a severe lack of oversight or transparency in data treatment practices (Keating 2013). People around the world were shocked and felt betrayed by companies which had supplied the NSA with data resulting in a flurry of research and opinions on rebuilding consumer trust in the “post-Snowden world” (Holmes 2013).

This example represents the first dimension of privacy regulation; where a government may justify the "violation" of an individual's privacy for their own purposes. While this dimension typically operates at the national and international level, what it
demonstrates is how multi-faceted many instances of digital privacy can be. Here an expectation of privacy has been violated by users around the world on multiple levels. Both the USA government’s sanctioning of these actions and the compliance of the implicated digital services to supply their data change the scope of the audience allowed to access this information beyond users’ expectations/understanding. From the initial point of data collection for profit, user information has been repurposed a second time. The matter of digital privacy then becomes subject to multiple layers of law: those that regulate the initial collection/use of information under economic models of contract law, self-imposed regulation of government in matters of security and international concerns on all fronts including the treatment of personal privacy.

Yet, within the PRISM program, the additional privacy concern prompted by the cooperation of US-based corporations supplying their data without notifying users puts forth a second dimension of privacy regulation; where the role of governance is expanded towards regulating the capacity of how services can treat user data in respect to the demands/desires of its people. This dimension operates in regard to the market and its providers. PRISM is only one such matter oriented far more towards the national-international level. Stark examples of differences between user expectations and the commercial realities of contracted privacy can be easily found at the more personal, individualized, state. The following are only a few prominent and well-documented cases which exemplify the importance between relations of law, commerce, social expectations and growing technical capacities.

In February 2012, the father of a young teen was outraged when his daughter received personalized coupons for baby supplies. To his own shock, the American retailer, Target, had actually discovered his daughter was pregnant before he did. By tracking her shopping habits, Target's statisticians were able to connect enough data points to reasonably assume she was expecting. In an interview this statistician, Andrew Pole gave a startling statement: “We are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy” (Duhigg 2012). This quote reflects a disconcerting reality about the current protections afforded by privacy law and the threat of potential invasions of privacy: within commerce it can be an acknowledged and exploited fine line.

Two such cases can serve as examples detailing just some of the ways contract law enables questionable practices. In 2011 Apple Inc. was sued in a class-action lawsuit by
Phone and iPad owners for invasion of privacy and fraud when it was discovered that the devices actually collected and stored up to a year's worth of locational data, despite a lack of notification nor the ability to cease the data collection (Christiansen 2011). Then, more recently, when an academic study on emotional contagion in social-networking sites was revealed to have collaborated with Facebook.com, manipulating the news feeds of 689,003 users in order to show how disproportionate amounts of positive or negative messages could alter user moods (Kramer et al. 2014), public outrage ensued. Because of this single study, both academia and Facebook came under heavy public criticism. Users of the service felt wronged and related themselves to “lab rats” subjected to an experiment they had not knowingly consented to (Goel 2014). Both of these cases demonstrate some of the many issues surrounding the collection and use of personal data where reality commonly exceeds the expectations an end-user.

These expectation thresholds are surpassed not only in the legal exchange/sale of user-information but also in the capacity of exchanged data to be related directly back to end-users outside of the contexts in which it was generated. This quality of digital information, capable of being stripped of time and initial context, introduces yet another facet to the complexity of digital privacy, this time emphasizing technological advancement. It is in this manner that privacy becomes somewhat synonymous with anonymity (a matter discussed later on in Chapter 7), where the ability to be private in a digital world is directly related to one's ability to not have digital information linked back to their physical identity. However, graduate student Latanya Sweeney found that 87% of the U.S. population could be uniquely identified simply by aggregating accessible lists of ZIP codes, gender and date of birth; information which could be bought by any interested person or company with the funds to do so (Sweeney 2000). Furthermore, additional data regression techniques have been used to re-identify individuals from information thought to have been “anonymized” by supplying services. In one such case re-identification was made possible by coupling anonymized medical records with seemingly unrelated movie rental information bought from marketers and generic data found on subjects available through online searches (Anderson 2009).

Possibly even more shocking is the array of information which can be assembled yet still considered “anonymous” by legal standards. Online advertiser and tracking company RapLeaf Inc. was able to compile a database containing over a billion e-mail addresses with attached profiles built from publicly traded data including information from Facebook, Flickr,
Friendster, Twitter, Pandora, Wordpress, MySpace, Bebe, Tribe, LiveJournal, Yelp, LinkedIn and Amazon accounts. Although “black-boxed” with no real names attached, these detailed profiles even contained information pertaining to voter registrations, shopping habits, real estate records and an assigned numerical measure of each individual's networking potential (Shaw 2010). Thus, as previous studies have already demonstrated, with this degree of information it would not be, in all likelihood, difficult to reverse-identify users from this data. Privacy concerns can thus become directly related to seemingly harmless individual pieces of information which, when put together over a period of time, become increasingly personal and identifiable.

These examples illustrate a disjunction between web-services and their user over an awareness of how data will be collected, treated and used. Within our present society digital information can be collected imperceptibly, easily stored in vast databases and utilized in ways which cause pervasive levels of personal and economic discomfort. This is all accomplished online under the legal protection of user consent via terms and conditions of use. Under the conditions of being digital, privacy demonstrates clear and strong ties between not only social and legal domains but an emphasis on economic and technical fields. These conditions are how researchers have qualified digital privacy as a unique phenomenon from other notions of privacy precisely because there are apparent failures in the rationality of end-users not seen in the physical world caused by the peculiarities of a digital context.

3.4 The Struggle of Research

3.4.1 The Problem of Putting the “Digital” into Privacy

This review has supplied a synopsis of some of the most basic elements which have given rise to the complexity surrounding a notion of digital privacy. Informational capitalism provides a groundwork for establishing value in the data produced by users visiting/using a digital service. Data-based subscriptions exist as a dominant economic model for free-content by exploiting this principle. Data, as a unique form of information, can then be utilized both as a commodity for direct sale and as method for generating profit through targeted advertising. This process is dictated by the terms and conditions users must accept to use a service. As legal documents, privacy policies detail a binding contract within a legal regulatory framework enforced by governments in which a service can redefine what is to be considered private information versus the property that free-content for-profit services derive
profit from. The disjuncture between the expectations of end-users and a servicer establishes the baseline for what can be conceived of as privacy concerns against the backdrop of actual privacy harms and privacy regulation. With every element functioning from the individual to global scale, the issue of defining concise subject matters for digital privacy discussions have been highlighted and the struggle is now clear.

Digital privacy is a complex system relying upon an examination of society within the spheres of economics, law and technological developments not only on the subjective individual level but corporate, national, trans-national and global scales. Because of how interconnected these various elements are, researchers have emphasized how situations of online privacy are inherently unique due the conditions which gave rise to them. Subjects in digital privacy research can analyze the economic principles of data-based subscriptions, terms and conditions as a means of achieving rationality, any related legal frameworks, the social perception/implications of privacy on various scales and/or the technical infrastructure which has given rise to the system as a whole. Thus, we find the complex web of rationales used to evaluate digital privacy with various degrees of emphasis subjective to the interests of each researcher. However, what is not recognized in this literature is how digital privacy and earlier notions of physical privacy/general privacy are the same. Hence, we arrive at the aims of this study, to find a manner in which this digitally oriented privacy research can fit within its preceding knowledge. That is, to provide a coherent manner of organizing existing discourses on privacy.

3.4.2 The Need to Move Beyond Economics

What has arisen from the general discussion of digital privacy concerns is a problem related to the scope and scale of relevant topics. An accurate conception of privacy, at least on a generalizable level, must be capable of explaining all of the aforementioned issues while also being capable of identifying why they have been treated as unique to digital contexts. Yet, few scholarly materials have even attempted to do so. Instead, they fixate upon particular issues subsumed by a notion of privacy that is either physical, digital or loosely categorized as general. In effect, existing research and the utility of its findings are very limited. This limitation is the result of their inability to produce an understanding of privacy as a concept. Unfortunately, current research ostensibly amounts to merely the situations which give rise to privacy.

If digital privacy is, in fact, limited to its unique relation with the domains of
economics and technological development, a great deal of insights can be drawn— as existing research has adequately expressed. However, life itself, even online, is not limited to these domains. Digital privacy concerns are not exclusive to consumer activities nor the rational evaluation of costs and benefits. For example, in the cases of cyber-stalking and cyber-bullying, there is, at best, only a weak correlation between consumer services and attached concerns. While the burden of notice and prevention could be placed upon services, like those of social media, to identify and stop such activities, this would cause other problems regarding the surveillance of user activity resulting in a similar problems as demonstrated by the NSA's PRISM program. Meanwhile, this potential solution would also loose sight of what assumptions actually makes this problem one specific to digital privacy. In this regard, although the rise of Web 2.0 and data-based subscription services have dramatically increased the production and subsequent collection of data, it is not possible to identify systems of e-commerce or the enabling technologies as the root of digital privacy concerns. After all, a model of privacy based on the issues surrounding e-commerce is, at best, only addressing a particular setting of privacy. Desires for privacy did not emerge from societies moving towards the digital age. If privacy existed prior to our own technological advancements then our treatment of digital privacy must also be understood not as distinct but derived from our social history.

Our failure as researchers to establish this principle is evidence of the failure of academic discourses in the natural and human sciences to recognize the necessity to reformulate the foundations of its own discourse; especially in regard to how the technological conditions of a contemporary society have fundamentally altered how one is to conceive of, and thus frame, the study of privacy online. Although scholars conduct their research within and for their respective disciplines, drawing assumptions from the history of their own fields and latent knowledge of others, there will be times when it is necessary to go beyond the apparent situational complexities. Therefore the nature of the scholarship must not be exclusively grounded in those situational complexities. By ignoring this, inter-disciplinarity and cross-disciplinarity remain sources of disjunction in privacy discourses. Due to the absence of a common and accepted theoretical foundation for the conception privacy there is no ability to relate various conceptions back to each other, despite addressing the same topics. It is this very problem that this exploratory study hopes to address, if not alleviate.
3.5 Concerning Media & Communication Studies

In disciplines such as Media and Communication Studies, which hold an inherent interdisciplinary perspective, the value of creating a unified theoretical foundation for privacy is more readily apparent. Mass communication, enhanced via the use of digital media, relates directly to concerns of digital privacy which currently stand in contrast to general/physical understandings. Privacy holds a central role in the act of communication by providing an understanding of audience and boundaries. However the veiled obscurity of contracted privacy in data-based subscription services poses a significant challenge for study.

Privacy, as a subject of study, presents researchers with the disjunctures, elaborated upon earlier in this chapter, should they choose to take an interdisciplinary approach. For disciplines like Media and Communication Studies ignoring the roles of politics, law, economics, social settings or otherwise is to leave out a key elements of thorough research. Left without the ability to choose a single domain to approach privacy exclusively from, a researcher of media and communication studies is then forced to relate disparate research without a clear way in which privacy can be operationalized.

Take, for instance, the issue of comparing the ways various online services treat user data. The central goal of such a study is to compare what information is regarded as private, in what ways other information is commodified and how aware users are of these actions. The obvious choice is to turn towards privacy policies and end-user agreements as the contracts which dictate these terms. However, here lies the problem. How does one actually operationalize privacy in this regard? There is no straight-forward way. Some studies choose to this form of privacy as levels of user competence and comprehension thus they operationalize privacy as a content analysis of terms and conditions via rhetoric, length and accessibility. Others utilize surveys but face the issue of overcoming the subjective nature of privacy. Still, other researchers evaluate online privacy in terms of a fair exchange for access to goods/services. There are the legal, political, cultural and social factors to consider as well. Without one clear manner to conceptualize privacy there is no singular way to operationalize it, in any context, while being capable of recognizing the limitations of that particular operationalization. Furthermore, to then simply merge other perspectives one is at risk of fallacy due to unrecognized differences in assumptions.

The ambiguity of privacy also serves as a problem for media researchers as a matter of ethics. In the Kramer et al. (2014) Facebook study a matter of ethics surrounding privacy
erupted as the public became aware that they may had been subject to emotional manipulation. Consent was the pivotal issue. When conducting research on specific mediums and their users, scientists face a question of what represents public information and what requires consent to use. For Kramer et al. their study utilized an extension of Facebook.com's Terms of Service as a means of formal consent. Users, however, were not explicitly aware they had agreed to such a possibility. Negative recourse occurred because users' news feeds and posts were monitored/manipulated without their explicit knowledge. Legally, this study was permissible but ethically it encroached upon subjects' personal privacy. Because we lack a clear understanding of what privacy is, these types of misunderstandings pose a growing risk for the public reputation and trust of researchers. By creating a theoretical foundation for privacy, researchers, regardless of their field, could garner a stronger understanding how privacy relates to their research and subject matter. Understanding what privacy is at its core can help researchers foresee any potential ethical concerns and take the necessary steps to avoid any possible misunderstandings over what is to be considered private on digital media, necessitating explicit consent.
Chapter 4- Research Problem & Questions

The research problem for this study lends itself to the issue of establishing what the sub-theoretical notion of privacy is. This in turn renders it possible to accommodate the totality of existing research within a unified theoretical platform. To do this, I focus on one primary research question and three subordinate research questions:

R1: What is privacy as a sub-theoretical notion?

R1.1: What distinguishes general privacy from other forms?

R1.2: What distinguishes physical privacy from other forms?

R1.3: What distinguishes digital privacy from other forms?

To answer these questions requires the identification of what topics are involved in the academic discourses which surround general, physical and digital privacy and the manner in which they are discussed. This process of identification, carried out by the structural-content analysis, enables the recognition of patterns which are common across the various conceptualizations of privacy. Utilizing the knowledge of what elements compose these conceptions, the analysis can continue by then examining the underlying assumptions contained within any discovered patterns by further reducing any one concept down to its composing signifiers (i.e. what is being measured). In doing so, it should then be possible to see what, if any, qualities of privacy are truly common regardless of situational contexts; thus providing an answer for how technological developments have altered these fundamental notions to such an extent that it has seemingly situated digital privacy as an altogether unique conceptualization in relation to general and physical privacy.
Chapter 5- Methodology

Throughout the course of this paper many allusions have been made to the concept of a 'sub-theoretical' notion (STN) and to a structural content analysis (SCA) jointly as a means to arrive at a theoretically unified conception of privacy. With both the STN and SCA as emergent methodologies in the field of sociology, this analysis will now clarify precisely this analytical method both in regard to its object, its justification as a methodology and its application to privacy discourses.

5.1 Analytical Method

5.1.1 The Sub-theoretical Framework

The term “sub-theoretical” is not entirely new to academic discourse. A thorough search conducted amongst literatures can reveal its brief mention or usage, despite the absence of a substantive definition to qualify its use. Alvin Gouldner, in seeking to establish a “sociology of sociology” commonly referred to as “reflexive sociology”, provides one of the must definitive early explanations of the sub-theoretical in his book *The Coming Crisis of Western Sociology* (1970). He defines the sub-theoretical as the 'infrastructure' or 'assumptions' all theory is based in. Building from a phenomenological standpoint, Gouldner elaborated that 'theory' itself is not just merely influenced by social structures but produced from them. In effect, the sub-theoretical becomes the domain of all the assumptions and sentiments which both liberate and constrain theory (Chekki 1987, 19). However, Gouldner's overall purpose leaves the sub-theoretical incomplete as an analytical tool by limiting its development to the establishment of reflexive sociology.

In Michael E. Brown's book, *The Concept of the Social Uniting the Humanities and Social Sciences* (2014), he undertakes the strenuous task of not only elaborating on the definition of sub-theoretical but actually employs it, as an analytical tool, to analyze the very foundations of the human sciences. In a sense, Brown builds from this small existing body of knowledge but pursues a far richer analysis of the sub-theoretical by questioning the very nature of language, using both broad philosophical and specific epistemological foundations, to critique the production of knowledge itself. At its very core, his work then draws out the distinction between notions of rationality, represented by theoretical development, and human nature to a depth not yet achieved by other scholars.
Brown establishes a sub-theoretical notion to be something both irreducible and irrepressible in the activity of life which is apparent across all human sciences. Thus, in seeking what this common object is, shared by all the human sciences, he finds the capacity of the sub-theoretical to unify academic discourse theoretically into a single field (2014, 2). To this extent his book is able to identify sociality as the unifying sub-theoretical notion for the human sciences as a whole. Sociality when viewed as a sub-theoretical notion, as demonstrated by Brown, is:

...[first] taken for granted as logically prior to prevailing theories and as the ultimate object of theoretical concern; second... is radically transformed by its standard representations into something altogether foreign to its logically prior conception; and third, that there are significant consequences of returning to that sub-theoretical conception for our very notion of theory no less than for formulating and evaluating specific theories. (ibid.)

In this capacity, Brown manages to employ a functional definition of the sub-theoretical to clarify the social as a common object across seemingly disparate disciplines. He combats current ideologies to ground theory in how the world is as opposed to how people think it is, which is elaborated later on as the product of theorizing.

This argument is constructed so meticulously, with very specific articulation and phrasing, that reproducing the intricacy of his argumentation in summarized form becomes a very difficult task to accomplish. Immense effort has been taken so that the remainder of this section can provide a brief of Brown's arguments, insofar I have interpreted them as relevant to my own application of the sub-theoretical notion within this project. It is thus important to note that while Brown sought to unify the human sciences, this study aims at a much smaller, and therefore simpler, application of the sub-theoretical to examine the existing conceptions of privacy. Brown was required, by the nature of his argument, to consider all established literature and existing theoretical frameworks across every discipline in the human sciences. For validation, his development of sociality as a unifying sub-theoretical notion had to hold true across every possible application. I seek to only analyze the conception of privacy, a single conceptual object, across academic discourses and need not examine the disciplines themselves. As such, I do not utilize the entirety of Brown's argument about the divergence of the human sciences but instead, focus my employment of the sub-theoretical specifically within Brown's critique of the relationship between the
'activity of theorizing' and the 'production of theory'.

It is here where Brown defines the origins and qualities of the sub-theoretical as an analytical tool used to evaluate the logic contained within conceptual development. Although emanating from Gouldner's definition, Brown's work is predominantly epistemological, thus granting a degree of generalization which removes the limitation of the sub-theoretical to any one particular field or subject. The goal of utilizing the STN is to demonstrate how a concept, such as privacy, becomes continually refined/purified through attempts to reduce its ambiguity; but, in doing so, looses its significance to the realities of social life, motivating the need for the sub-theoretical analysis to make the initial conditions which brought about the desire for refinement intelligible again. In doing so, it is then possible to identify a concept's meaningful application to human affairs beyond what its developments have attempted to circumscribe.

To show what produces the sub-theoretical, Brown begins with the epistemological concerns surrounding production of knowledge via the process of producing theory. This begins with the separation of the activity of theorizing from its ostensible product, theory. Theorizing, as a process, arises from an object of ambivalence and/or ambiguity. When one finds such an object they seek to generate a theory which can reduce this ambivalence/ambiguity through the use of signifiers which are assigned “value” to provide a concrete explanation (Brown 2014, 133). Put simply, the goal of theorizing is to produce theory that is capable of providing a justifiable explanation for the addressed object/phenomena through its signifiers. Signifiers thus act to reduce ambiguity by representing its ostensible elements, or measures, of the original theorized object. To this end, theory ultimately seeks to create a perfectly signified idea, absent of subjectivity, while retaining the capacity to explain itself. **Herein lies the problem found by Brown.** Theory seeks, during the course of theorizing, to become something that eliminates the very ambiguity which generated, and therefore justified, the conditions for theorizing the object in the first place. This quest for purity, inherent in theory, results in a theory which cannot justify itself – loosing what is “human” about human affairs. That is, affairs of abstraction which have little to do with their own genesis. This is what Brown considers to be agent-independent reality.

The theorizing object is re-presented as a concept, a purified signifier, in theory. Without careful attention, these concepts loose the quality of life which made the logical
conditions of theorizing intelligible; the object of theorizing is changed within the purification of a theory from what it is, the conditions of life, to what it does, the activity of signifying (Brown 2014, 133). Brown's sub-theoretical notion is thus defined by the conditions of life which brought about theorizing— the irrepressible pre-conditions of theory on which theorizing ultimately depends. In his analysis of theoretical progression, he then recognizes that the life of theorizing becomes accounting for concepts by their formal relations with other equally degraded (refined) concepts (ibid., 134). Hence, as the process of theorizing develops in succeeding theories/theory, “it builds upon the theorizing subjectivity by the subjectivity which is no longer motivated by its material” (ibid., 135). Consequently, theory finds itself in a conundrum regarding its sub-theoretical object.

As theory is refined by its own ostensible product, it moves further away from, but ultimately relies upon, the original sub-theoretical object as the conditions which gave rise to the activity of theorizing, e.g. the original concept itself. This occurs when a finished theory ignores the 'activity' of how it became a theory by regarding the activity itself as the theoretical object— thus being unquestionable (ibid., 140-41). In effect, the capacity of theorizing can actually be considered to be self-motivated, as if it were trying to constantly find itself. In an example, he points out the progressive refinement and use of the commodity concept. The use of commodities as objective (a theorizing subject) is only possible within a universe of exchange thus a commodity “cannot account for itself (be accounted for) as a product and, therefore, cannot teach what is involved in arriving at what it has become” (ibid., 133). In essence, as the concept of a commodity is continually refined and used throughout academia it becomes an unquestionable element of its derivative theories; yet a commodity cannot exist outside of a social system of exchange. The STN of the commodity concept makes the set of assumptions current forms fail to recognize intelligible again.

The commodity concept results in what Brown describes as a failure to be progressive. By not recognizing its obligation to the activity that is both its condition and its object, theory fails to root itself in the actual conditions of life. Viewing these conditions, as the sub-theoretical object for study, Brown recognizes that to study the sub-theoretical is analogous to studying the 'life of the concept'. This means attending to what the theoretical object is not – what the developed signifiers have left out in-order to produce a purified concept. Re-engaging with what was left out of the theory thus allows the reflexive activity of theorizing to uncover the suppressed history of the concept through an acknowledgement of
its reification (ibid., 137-39). This is a return to ambiguity and subjectivity in order to describe the conditions of life prior to its refinement as a concept. This is accomplished by analyzing the relationship between a concept and its object (theorizing versus theory), where “the activity of the sub-theoretical object, its force, remains both the occasion for and the material base of theorizing” (ibid., 143). As such, Brown describes a sub-theoretical analysis as requiring theory to “submit itself to the very questions that give rise to theorizing” (ibid., 147).

It is now clear that the complexity of Brown's argument is a product of necessity regarding the scope and depth of his claims. While Brown is writing against the backdrop of Marx's response to German idealism and subsequent critical thought, it might be useful to see his attempts to essentially define the critical method itself as related to the work of Thomas Kuhn. Brown's work has strong philosophical overtones and seems to reflect a particular dimension of Thomas Kuhn's paradigm or “framework” which lays out the shared beliefs governing the processes of normal science. By Kuhn's standards, what Brown puts forth via the STN is 'revolutionary science' by seeking to revise existing scientific practices and beliefs. In this way, Brown's critique of the process theorizing and the production of theory constitutes a critique of the practices of normal science in the production of scientific truth. By highlighting how our existing scientific frameworks have failed to allow adequate communication of social reality, Brown is thus employing the sub-theoretical to present a new method for viewing social reality, in effect, altering the perspective of scientific truth. He rejects such notions as Feyerabend's theory of proliferation by demonstrating how constant theoretical growth in fact entrenches scientific truth into a single scientific reality further distancing itself from the social reality of actual life. To this end, Brown's work places a great deal of scientific knowledge at stake by questioning ideologies' accepted notions of truth. These accepted notions are grounded in how academia thinks the world is as opposed to how the world actually is. Therefore, I do not find it unreasonable to presume that Brown's work is indicative of a call for a paradigm shift, by seeking a return to the “life of a concept” when theorizing. However, this explicitly places Brown's work against mainstream science. It is therefore reasonable to anticipate a great deal of resistance towards his ideals.

It is certainly possible to critique the philosophical and epistemological claims Brown makes in his book, however, such critiques are rooted more in the manner of how he has framed his argument rather than in regard to his analytical tool, which is a sub-theoretical
notion. The sub-theoretical, for this study, is ideal for determining what a functional conception of privacy is precisely because the sub-theoretical notion is designed to examine how a concept has developed in its refinements—looking not only at what is present but emphasizing what has been lost as it is reduced into more perfected signifiers. For this project, Brown's sub-theoretical notion describes the exact analytical tool necessary for analyzing the conception of privacy from its general application in broad and/or physical contexts towards its refinement to fit digital contexts at a level of analysis which can negate both interdisciplinary and cross-disciplinary differences.

Whereas Brown's work required the analysis to focus on established theory, this study derives its focus from the very lack of a coherent theory on privacy since this lack of coherence is directly related to the struggle scholars have in reducing its ambiguity. This makes my own sub-theoretical analysis much simpler by allowing me to directly study the conceptual developments of privacy and their associated signifiers in non-theoretical texts, with a much smaller degree of distance from its sub-theoretical object. Furthermore, it allows this study to circumvent the more controversial notions surrounding Brown's epistemology. Since the object of this study is itself, a concept, I do not need to question the validity of any theories nor the qualifications of privacy-related knowledge. Instead, I only need to analyze how, within established discourses, the relationship between privacy's conceptualizations and its signifiers have changed. In addition, the clarification of how the sub-theoretical notion is explicated also explains why theory itself cannot be a starting point for this study since theory itself is based on and, problematically, detached from the sub-theoretical. Theory, for this project, is not a molding force but an object of analysis when present.

Hence, in seeking what has changed and what remains irreducible as the sub-theoretical notion, two conclusions can then be drawn. First, the sub-theoretical notion itself will reveal the initial conditions of social life which gave rise to the desire to conceptualize and refine privacy through the activity of theorizing. In this regard, the sub-theoretical notion's significance is found in that it establishes the foundational material for theory by making it intelligible. Second, the refinement of privacy's signifiers, with respect for and in contrast to digital contexts, should themselves provide insight as to how digital contexts specifically altered the social conditions surrounding privacy. My application of the search for the sub-theoretical in principle aims to identify and preserve the essence of ambiguity in privacy which gave rise to the initial conditions of theorizing as explained by Brown. The
potential significance of these findings are to allow theoretical development, and consequently conceptual development, to acknowledge the theoretical foundations of privacy. And it is because of this acknowledgement that these conditions require the recognition of their universality; with the qualification that they are universal only \textit{insofar} as they are what establishes the human element prior to its refinement within a particular field or perspective.

5.1.2 Using Structural Content Analysis

The way to arrive at the sub-theoretical notion of privacy is organized via a structural content analysis. A structural content analysis (SCA) is derived from methods of critique, content analysis, formal sociology and methods of the field (Raphael, Hooiveld & Manning 2014). Fundamentally, a SCA is a variant of traditional qualitative and quantitative content analysis techniques building from, as any form of content analysis does, the premise of taking certain signs, typically words, and assigning them to content categories in a process of coding but is specifically capable of handling situations where codes and variables occur multiple times in a different relationship with the text (Isberg et al. 1972).

As such, the primary use of a structural content analysis is for the analysis of complex systems to develop a representation of the relationships between elements contained in the texts with particular attention paid to the definitions of governing rules (Breakwell et al. 2006, 293-94). This can be accomplished by examining the literal elements of the texts and analyzing how it has been formatted to communicate specific ideas (ibid.) – so called 'reading how a text is written' (Brown 2014). The aim of a structural content analysis is to act in contrast to modes of data analysis that take their purpose as either causal or interpretive forms of explanation. By seeking the interrelations amongst selected elements a structural content analysis is, by its nature, an inductive methodology. Structural content analysis is thus an ideal exploratory method for the application of Brown's sub-theoretical notion by establishing a method for analyzing the complexity of relationships established under the various conceptions of privacy in order to extract their intrinsic qualities.

Since this is an exploratory study, it is useful to clarify some of the epistemological assumptions of an SCA. These epistemological assumptions deal with (1) the purpose of analysis; (2) the validity of data; and (3) the role of the sub-theoretical notion. Raphael, Hooiveld & Manning (2014) note that SCA, or at least their incarnation of it, aims to produce an ‘empirically grounded critique.’ They hold this to be in stark contrast to other qualitative projects where the aim is to produce interpretive explanation, with Grounded Theory projects
serving as one of their examples. In their explication of what precisely an ‘empirically grounded critique’ is, they first define critique as “a mode of data analysis which often involves ‘verbal slights of hand’ in dealing with abstract concepts.” (ibid.) They argue from this starting point because of how ‘critical explanations’ tend to be respected for their strenuous effort, but, at the same time, discarded in terms of a critique’s validity as a form of scientific inquiry. This is where popular notions of “armchair sociology” are invoked – where the ‘armchair’ makes reference to how critique often fails to ostensibly gather any significant form of data, instead simply relying on the work of others.

Although Raphael, Hooiveld and Manning recognize there are plenty of cases where this is indeed true, they reject the notion that critique, as the main feature of the critical method, is not empirically grounded – when done properly. SCA, in its most basic form, first establishes how things stand and then proceeds with either a positive or negative critique. However, before clarifying the positive or negative critique, they also draw on Raphael’s earlier work to establish what is qualified as ‘empirical’. Through his work on the development of an interpretive sociology, Raphael (2014b) held that the mere presence of many orders of abstraction does not negate the ‘groundedness’ of data; rather, this ‘empiricality’ is only negated between classes of orders of abstraction which can only be shown through critique. This is to say that a structural content analysis can be qualified as “empirical” because it is uniquely geared towards revealing the ways in which other research may have confused various levels of abstraction (refinement) by assuming their conceptualizations are rooted in the actual conditions of life rather than other degraded concepts, such as markets. With that key assumption stated, what is either positive or negative about the critique can now be clarified by its focus: the focus of a structural content analysis is either to (a) positively emphasize a sub-theoretical notion whose empirical evidence is consistent across orders of abstraction because those orders of abstraction, and their contents, depend on that notion through the course of activity that their claims depend on; or (b) negatively emphasizes how that sub-theoretical notion fails to cross the classes of orders of abstraction.

With the epistemological assumptions of SCA summarized, its implementation in this study can now be stated. Given the primary research question, this study aims to extract a critique of the conceptions of privacy rooted directly in the structural content analysis of texts as the empirical subject. This will be done by analyzing the underlying relationships between
the higher and lower elements of privacy through a process of “coding” the texts where each set of elements will, eventually, produce its own sub-theoretical notion. In this sense the higher elements of privacy become the very conceptions of privacy itself while the lower elements represent the many signifiers used under these conceptions. However, deriving these two STNs requires a multi-tiered process of reducing the texts to their structural elements. This is done by continually breaking down the structuring of a text until the “codes” themselves provide an identifier for the level of abstraction contained within the text. These levels of abstraction represent how far along in the continual refinement of the conception of privacy each element is. In identifying the various orders of abstraction contained within the texts, it is then possible to see how all of these orders fit together. Taking these levels of abstraction and situating them into this hierarchical order permits these two sets of structural elements to be established within the greater levels of underlying logic contained. A clear “life of the concept” emerges and this then provides the opportunity to formulate a model of the sub-theoretical notion contained within each set of structural elements; and as this clarity is obtained to the brink of ambiguity, the sub-theoretical notion of privacy emerges along with the associated digital privacy dilemma. In this case, because the sampled texts produce a framework which allows further sources of information to be grafted, the structural content analysis becomes its own secondary form of a literature review based on the conceptualizations and applications of privacy, precisely because the SCA informs how the literature is to be discussed in a comprehensible manner by extrapolating the orders of abstraction.

5.2 The Sample
The aim of this study is to draw conclusions based on what can be considered a representative sample of privacy literature. A set of 28 books/edited collections were selected using purposive sampling based on the qualitative assessment of each book's relevance to the discussion of privacy. This selection was based from an original assortment of texts queried by searching across Uppsala University and Northeastern University libraries' catalog indexes for the terms “privacy”, “privacy online”, “digital privacy” and “internet privacy” over January 2014. Selections were made if, from the book's title and table of contents, it was inferable that the criterion of the book centered around a detailed discussion of privacy or a summary of the facets of privacy—these indicators served as a prima facie case (See
Appendix A for a bibliographic listing of the selected texts). Time constraints limited this sample, thus an upper boundary 9,000 pages was established. Once the total page count was over 9,000 the sample was considered adequate resulting in a text corpus of 9,184 pages.

To a certain measure it can be inferred that this method of sampling was also one of convenience, thus resulting in a limited measure of generalization. I refute this claim based on the abstracted nature of the topic and nature of the sub-theoretical notion. To ensure that any derived sub-theoretical notions were in fact capable of not only explaining digital privacy but privacy at its core it was necessary to permit the representation of literature outside of, and including, dominant discourses. To establish a sample based on any strict criterium would limit the variety of opinions represented. Relying upon other traditional empirical criterium, such as citation rates or other measures of popularity and/or the representation of specific specific sub-subjects, the sample would have been faced with numerous other potentially limiting factors. Citation rates are subjective to the platform's counting processes and could be biased based purely on the prevalence of a specific sub-topic within privacy literature. Furthermore, as this sample addresses the notion of privacy both as an overall concept and seeks the largest possible scope of its perceived digital contexts, there was no one universal search term available nor a complete index of possible texts to generate a simple random sample from.

Selected texts needed to reflect, to highest degree possible, all dimensions of privacy from field of study (e.g. economics, law, social sciences and information technology) to topic (e.g. surveillance, tracking, e-commerce, governance, data-mining, etc.). As a consequence of this complexity, it was most ideal to set the least amount of limiting factors possible. Thus, with such a complex topic, it was found that a general purposive sampling was best suited by allowing for a measure of researcher subjectivity in the selection of texts. To compensate for possible selection bias, the sample size was increased to the largest possible degree while remaining manageable. However, one of the fundamental assumptions a SCA makes is that the sample does not contain any invalid data. This is the predominate risk of error within the study. Should any one data point not fit into the sub-theoretical notion or appear as a theoretical outlier then it must decided if (a) the sample contains theoretically/conceptually false data or (b) the derived STN is incomplete/wrong. Unfortunately, to encounter this problem requires the selection and analysis of the texts already. Readers are reminded that, in hopes of avoiding any such issues, the sampled texts had been published and chosen from
academic library catalogs.

5.3 Description of Selected Texts
In order to consider the selected texts representative of privacy-related discourses, as a whole, I have stated they must, to the fullest extent possible, reflect all the dimensions which compose the complexities of this research. Simply qualifying the texts as related to privacy does not provide the necessary validity to make these claims. However, since a single text can present many different topics, as well as ways to approach these topics, the accurate description of each text poses a significant challenge – the only uniform categorization is privacy itself. To resolve this issue, the use of purposive sampling enabled the selection of texts across the widest variety of genres and disciplines (See Appendix B for a complete table of each book's genre and primary discipline(s)).

5.4.1 Represented Domains
As explained in Chapter 2, there are four primary academic domains involved in privacy discourses: social sciences, law, economics and technology. Nevertheless, these domains are not mutually exclusive when discussing privacy. Although each text can demonstrate a specific orientation/emphasis it is highly unlikely that there would be no mention of a topic relating to the other domains. While this can pose a significant challenge when attempting to categorize any one text, I have chosen to simplify the matter by taking into consideration only the primary orientation of each text as a whole demonstrated by the sum of their contents and author(s) native fields. The results are shown below in Graph 5.1:

![Graph 5.1](image-url)
General texts refer to those which demonstrate no specific orientation/emphasis but rather a summary of many different perspectives and/or approaches when discussing privacy. These texts were primarily characterized by a specific orientation towards privacy itself rather than a specific discipline. The minimum requirement for this categorization was the inclusion of topics/discussions of at least three of the four major domains. When a selected text demonstrated a very specific orientation across two particular domains it was placed in its own category as a text which emphasized a specific interdisciplinary relationship in privacy-discourses. Of the six possible combinations then possible only three were found: Technology and Economics; Law and Social Sciences; Law and Technology. This means that no text in the sample demonstrated a specific relationship between Law and Economics, Technology and Social Sciences nor Social Sciences and Economics without finding other domains relevant the discussion in a significant manner when addressing privacy.

At first glance, it appears that purely technological or economic perspective on privacy is either under-represented or rare in occurrence. To find out if Technology and Economics were indeed under-represented in the sample a simplified distribution of the primary disciplines was created (See Graph 5.2 below). Once the frequency of each text representing two major disciplines was added to their core values a more even distribution was found. Accounting for the fact that the General categorization stands for the representations of least three major disciplines, no one domain shows a dramatically lower frequency.
5.4.2 Represented Genres

Genres of the selected texts were based on broad categorizations as seen below in Graph 5.3:

Textbooks \((n=6)\) were considered any book which offered a broad explanation of privacy without specific emphasis on a single topic or quality which was otherwise categorized as a Monograph \((n=5)\). A total of 5 texts were published collections of scholarly articles on privacy. The 3 texts categorized as Reference were designed to provide readers with brief overviews of specific topics with guidelines for further research. Popular texts \((n=6)\) were those which refrained from having a distinct academic tone, although this categorization ranged from the casual to more educational in nature. One text, Book #6, was a collection of legal case studies reviewing the legal frameworks various countries had established in regard to general and digital privacy. Finally, a total of 5 texts were categorized as Anthologies which contained chapters written by various authors organized under specific topics.

5.4.3 Determining Representation

In total the sample demonstrated a wide-range of both disciplines and genres on a generalized level. This study was limited in the sense that I had no clear way to establish parameters for comparison which could objectively measure the representativeness of my sample in respect to the totality of privacy-related research. Instead, the assumption was made that my sample is representative of the current state of privacy research given the basic measures of variety analyzed. Considering the ambiguity of the privacy, a more detailed analysis of each text's specific subject-matter is left for the structural content analysis in the following chapters. Successfully deriving the sub-theoretical notion of privacy is the ultimate
test of if this sample is in fact valid. By its nature, successfully deriving the sub-theoretical notion of privacy should not only function to describe the developments of privacy as a concept across these particular texts but be capable of describing any situation of privacy. The capacity of the final results of this study to be generalizable is thus the actual confirmation that the texts were indeed sufficiently representative to produce valid results.

5.4 Establishing Validity & Reliability for the Study

No previous research has attempted to investigate the underlying notions contained in discussions of digital privacy in a manner not already fixated within an existing notion of what privacy is or should be. In other words, the goals of this theoretical study are to examine existing privacy discourses without existing bias towards a particular conception or theory. Discovering the sub-theoretical notion of privacy and, by consequence, that which explicates why digital privacy has been treated as a unique form of privacy requires that both the conceptions of privacy and any related theories become the subject-matter of this study and not inform the study itself. Without available precedence and because this study both attempts to apply newly developed methodological tools, namely the investigation of sub-theoretical notions, through the empirical lens of an exploratory structural content analysis it is faced with compounded issues regarding validity and reliability measures. In order to minimize these concerns it becomes vital to understand how this procedure was conceived and carried out as my own adaptation of Brown's processes. I will try to be as comprehensive as possible while documenting the processes used to analyze the sample texts while also providing reflections on the experience itself so that this study may serve as a methodological pilot for any future research to build from.
PART II: The Structural Content Analysis
Chapter 6- Preparing the SCA

At face-value the 28 selected texts are nothing more than books which would normally be used to construct a literary critique or literature review. With a text corpus of 9,184 pages they also represent a superfluous amount of information surrounding privacy-discourses if all that is desired of them are their conceptions of privacy and related signifiers. It is neither convenient nor efficient to analyze the entirety of each book word-for-word in order to extract these few desired pieces of knowledge. Rather, this method often burdens a researcher with the arguments for valuing one conception of privacy over another or the particular contexts each is suited for. All of these matters fall outside of the scope of this study's aim. The design of this SCA is to exclusively detail the relationships amongst privacy and its signifiers in order to discover privacy's sub-theoretical notion(s). To produce the SCA, which organizes these relationships for analysis, every text must first reduced down into its empirical elements.

By reducing the texts to their structural components, thus limiting what is be analyzed to the way each text is composed, it becomes far easier to comprehend a large quantity of data from a perceptual distance sufficient enough to allow a researcher to see the various logical flows contained. In the structural content analysis these “logical flows” are represented by the headings each author uses to move from subject to subject-matter. Under the SCA, the level of each heading (i.e. “Section” → “Chapter” → “Sub-Chapter” → etc.) can be considered to generally represent a level of abstraction within the book. For example, Sub-chapters are higher orders of abstraction (more specific, thus farther from original ambiguity) than Chapters because within a SCA the sub-chapter is to be considered a “sub-topic” related the topic of the chapter itself. It is reasonable then to initially comprehend the process of creating a SCA as equal to the aggregation of individual outlines for each selected book to see how one point follows another, what connections are made in each argumentation and how a conception of privacy is related to specific topics which act as the signifiers for that form of privacy.

It can be argued, by using structural outlines of each text, this particular approach strips the books of their substantive content and the contexts which actually compose their justification. When using a structural content analysis however, the opposite is true. By increasing the level of analysis to the actual structural components of the selected texts, what
is removed is not the empirical subject-matter but the subsidiary information contained within
the assumed level of abstraction. This also provides a far greater level clarity to the critique
precisely because it unilaterally strips away any information deemed superfluous. Lowering
the informational barriers required for the exclusive study of privacy's conceptualizations is
exactly what makes the SCA an ideal methodology for this study. The goal of creating a SCA
is not to question the validity of the arguments contained within the data but to assist in
revealing any hidden logics the author's themselves were unaware existed. Subsequently, any
removed subsidiary information, although not used while creating the framework for the
SCA, can be revisited when the results of the structural content analysis are discussed as
evidentiary support.

In this capacity the structural content analysis of privacy is defined by two distinct
phases. First, the sample is broken down to produce a list composed only of structural
elements relating to privacy-discourses. This list can then be studied and used to produce a
code representing the summary of information contained in these elements. In return, the
codes present what should addressed in an analysis of privacy's life as a concept. With a
means of presenting the entirety of privacy-related discourses in a concise and coherent
manner, the SCA can then be seen as an informed literature review; where the codes become
the latticework on-which any additional information can be grafted. In this study three stages
of iteration were necessary to arrive at a point where codes could be produced. Each stage
was dictated by a set of rules which ultimately refined the initial text corpus of 9,184 pages
into a final sample containing 4,486 structural elements. Throughout the process, each
iteration was kept separate for reference and reliability checks.

6.1 First Iteration
In the first iteration of the sample an outline for each book was created by manually scanning
every page of text for headings. As traditional with any outline, every type of heading
(sections, chapters, sub-chapters, etc.) was transcribed with an increasing degree of
indentation representing specific levels/location within the text. Maintaining the levels
contained in each text provides a critical visual clarity for the identification of when certain
elements are considered by the author to be classified as elements under a particular notion,
theory or example. Starting at the main textual body no headings were excluded except for
those which existed outside of the core body of the book including table of contents,
The manual coding of the books rather than the simple extraction of the table of contents ensured that a complete mapping of the author's arguments was obtained. Of the 28 books, 21 (75.0%) contained sub-level headings not found in their table of contents. In some cases, when a particular book contained any graphic indicators which broke the text apart, such as spaces or numerical headings, but lacked an appropriate title one was created. This occurred sporadically amongst the texts in specific chapters, typically those written by different authors in an anthology. It was decided that since the structural equivalent of headings had been added but left without an actual title that in their place brief descriptions of each section were added after reading the entire section involved. Although the new headings were not from the original author they did not create any issues regarding the validity of the element because they still served the same empirical purpose: to represent the contained text.

By actively engaging with each text throughout the creation of the outlines this phase also acts as an introduction to the material in general. In this respect, while manually coding and scrolling through each book it was possible to skim and/or read actual portions. This process allowed for the first dataset to include a measure of personal notes and bookmarks for future reference in later iterations and while writing the SCA. In particular, this strategy was employed anytime a heading included references that were unfamiliar or ambiguous. An example is shown below in Figure 6.2:
Here in Book #18 in first chapter “Introduction” under the sub-chapter “Problem Definition” the 3rd degree heading “Three Causes” still leaves no evidence of its meaning regardless of its relation with other elements in the outline. By combining notes and knowledge of its precursory headings (“Privacy and Liberty”, “Agents and Interfaces”, etc.) an understanding of context and meaning is permitted.

The power of creating structural outlines of the sample texts becomes apparent when viewing the above sample. Without need for the literal text contained under these headings one is able to gain a sense of the logical flow the author utilized. From these sixteen lines it is possible to see how the author has related digital privacy towards notions of power, control and liberty. Furthermore, it is possible to tell how these signifiers have been addressed at the business, national and individual levels through social science and legal domains with cause related technological development. When applied to the sample as a whole, the scope and depth of relevant information garnered scales dramatically without having to be overwhelmed with the volume of text.

Comprehension of the sample materials was essential for the first iteration. Because this process is inherently subjective to the researcher, concerns over interpretive ambiguities are justified. Care must be taken to distinguish any notes from the actual structural elements of the texts so that they are not included in the count of empirical elements contained within the sample. Yet at the same time a concise level of detail, sufficient enough to provide
context, is required at any point where it is necessary to compensate for the individual limitations of a researcher's knowledge base. However, whatever personal bias this process entails is negated by the fact that this stage of establishing the SCA is designed to aid the researcher. Any actual empirical data (the structural elements, i.e. headings) will remain consistent. To ensure the initial outlines were free from coder error the entire process was done a second time using the first generated list to look for any missing headings and re-check notes. Overall, this accumulated into a measure of 11 missed headings. Once the second iteration was completed (see Section 5.5.2 below) to provide an accurate count of the total structural elements contained across the sample, an error rate of 0.23% was calculated and the decision was made to regard the accuracy of the outlines as reliable and continue on without doing additional checks.

6.2 Second & Third Stage Iterations

Second and third iterations of the dataset were restrained to similar rules as established by the first iteration to ensure no researcher bias could influence the total number of structural elements to be considered. These reductions were meant only to eliminate miscellaneous and redundant/non-informative elements. In the second iteration only the notes created for reference from the initial iteration were removed. This allowed for easier navigation and distinctions amongst the dataset as well as enabling the use of a text-line counter to provide a measure for the initial sample size of recorded structural elements (n=4,740). With this measure it was possible to calculate the error rate, stated earlier, from the initial coding to see if additional checks were required before proceeding to the third iteration.

The third iteration was the first application of reduction methods designed to “clean” the data. At this time any redundant and non-informative headings were stricken from the sample. The identified and removed headings were: References, Discussion, Introduction, Conclusion, Epilogue, Summary, Outlook, Limitations, Related Work, Future Work and Background – as long as they contained no additional structural information. Consider the following example for clarity:
When looking at “Conclusion” and “Conclusion: Toward an Ethics of Self-Restraint” the former heading is typical of one removed as it serves only a literary function, not holding any significance for the outline's logical progression. However, in the latter example the term “conclusion” merely precedes an actual element. In cases such as these, when generic and redundant terms were coupled with additional information not within a sub-level, their deletion would also constitute the loss of a unique element and were thus left within the sample. In the case that under one of these headings there were additional sub-levels, in order to maintain the integrity of how each data block as constructed, the supra-heading was not removed. In these situations headings which would otherwise have been removed did denote significance as a container providing context for significant sub-level elements.

To ensure reliability, once again, every stage of alterations were kept as individual files. Side-by-side comparison, when necessary, easily provided the full text's contexts. To ensure the reliability of this reduction process, it was checked a second time searching for the same elements. No errors were found and at the end of the third iteration, with the removal of non-substantial headings, the sample was reduced to n=4,486 structural elements. With the sample finalized, the formats of each structural outline were coordinated and combined into a single document. Although the final sample size does ostensibly amount to a large amount of information to consider, this is a remarkably smaller amount in comparison to the original sample of 28 books which contained roughly 12.6 million lines of text. Thus, when placed into comparison, it becomes clear how effective the process of creating a structural content analysis is at reducing the volume of information a researcher must comprehend.
6.3 Coding to Uncover Levels of Abstraction

At this point the structural outlines derived from the sampled texts have been reduced purely by basic methodological processes that contained only a limited degree of possible error or bias. However, as a raw sample of 4,486 structural elements related to privacy-discourses it is still not possible to produce a final structural content analysis in the form of an enhanced theoretically oriented literature review. In this form, the structural elements only display how each author has related and organized various aspects of privacy in their own work. As a whole, the sample remains disjointed. Resolving this disjuncture requires an active engagement and initial analysis of the elements to first identify how many unique elements there are and, secondly, the ways those elements are related. It is at this time, with the data in its most condensed form before losing substantive elements, it becomes necessary to begin a process of coding. This process was informed directly by the comprehension and overview of the dataset and indirectly by my own existing knowledge of the field.

The coding process began by establishing an initial set of assumptions. First, the dataset represents the authors' explicit or implicit intentions to provide order to their employed logics. Second, by association, the level of heading also indicates at what level of abstraction the content is considered to be; thereby establishing interrelationships amongst elements: sub-level (contained in), supra-level (contains) or of equal order (same heading level). Mentally re-framing the dataset to represent these notions creates the initial point for establishing orders of abstraction and their interrelations. As stated in the prior chapter, structural content analysis is not directly oriented towards the analysis of the arguments contained within the structuring (i.e. what is contained under each heading) but the logics informing them (i.e. how the headings and sub-headings relate and inform the literature's progression).

It also becomes relevant to consider that whenever complex materials are coded there is an intrinsic problem regarding possible bias or arbitrariness. In this case, issues could arise because the goal of coding the materials relies upon a subjective interpretation of the author's intentions to produce a logical flow. To limit any potential issues, a method of coding was required which could simultaneously breakdown each structural element into its most basic forms while accounting for the various ways privacy was discussed. This meant that the coding process would have to be dynamic enough to account for variances and redundancies in relations of privacy while specific enough reduce every situation of privacy into its
fundamental elements. With no clear answer nor precedence, arriving at such a coding scheme was a process of trial and error.

An initial attempt began with attempting to further reduce the third iteration of data. This meant taking single structural elements, accounting for their relations with those surrounding them, breaking them down into single elements and then describing those relations as a code. Issues with this process were apparent from start. Take the following excerpt from Book #1 in the final iteration:

| Figure 6.4: Complexity of Structural Element Relations when Coding, Excerpt from Book #1 | Chapter 1: Privacy-Enhancing Technologies for the Internet III: Ten Years Later |
| | 1) E-mail Anonymity and Pseudonymity Systems |
| | 2) Interactive Anonymity and Pseudonymity Systems |
| | 3) Communication Privacy Systems |
| | 4) Other Privacy-Enhancing Technologies |
| | i) Private Payments |
| | ii) Private Credentials |
| | iii) Anti-Phishing Tools |
| | iv) Useful Security and Privacy Technologies |
| | Chapter 2: Communication Privacy |
| | 1) Simple Proxies |
| | 2) Web Site |
| | 3) Local Proxies |
| | 4) Proxy Chain |

Immediately a desire to use aggregate terms for describing multiple single elements became desirable but even then there were issues breaking this outline down. “Privacy-Enhancing Technologies” (PETs) is the broadest element in Chapter 1 with “anonymity”, “communication privacy systems” and other specific technologies as part of its constituent relations. Yet in Chapter 2 “communication privacy” becomes higher order and its constituent relations become “proxies” (discussed as forms of anonymity granting PETs) and websites in general, a related topic which encompasses all other single elements listed. Even if each single element were initially coded as unique it was not possible to describe the complexity of their relations in a specific manner unless the context in which it was presented remained.

This issue persisted across all other types of coding then attempted. Once it was necessary to describe the relationships between various elements the shear complexity of these relationships compounded with varying degrees of abstraction presented across the sampled literature would become insurmountable. The only aspect which seemed to be working was grouping of single elements within each structural element under an encapsulating code. However, at some point in the process it always became apparent that
there was no single set of codes possible which could describe every difference amongst relations across each text/chapter. Albeit subject level, academic orientation, form of privacy or topic, at some point each coding term could not be expanded or utilized to describe every given situation of privacy unless that exact context became an independent code itself. What I encountered was the exact conundrum of privacy research I had identified: to describe privacy's relations with its signifiers I needed to maintain the context in which it was being presented.

A solution for this problem came from revisiting what the goal and purpose of a sub-theoretical notion is. The role of the sub-theoretical notion is to describe sum of all privacy's relations regardless of context. Attempting to create a coding scheme which retained contexts negated that fact. Therefore, in my attempts produce a structural content analysis which could do so I was accidentally attempting to bypass the very reason for using the SCA in the first place, as a way to provide a summary of all the relational dynamics discussions of privacy contain. It was impossible to code the relationships between privacy and its signifiers as they appeared in the texts as groups. Rather, the type of coding scheme necessary for this analysis required the breaking down context and limiting codes to elements which, when combined, could describe any one situation.

Instead of developing a single cohesive code which describes privacy, when seeking the sub-theoretical notion, process of coding requires the development of multiple codes which can encapsulate the highest level of abstraction for each component of the concept's relationships. Thus the appropriate process was based on the principles of dynamic programming, as a method used for breaking a problem down into its smallest components, allowing for the simplified analysis of a complex dataset and the employment of transitive logic. Beginning with the first book and continuing forwards, when an element representative of an order was considered to be sub-level to another they were merged as a single code under one order's category. If the element did not fit into any existing codes a new code was produced based on that element. This binary process of merging singular elements was used produce a basic coding scheme for the data, representative of any level of abstraction utilized in the discourses. A total of four distinct codes were created: type of privacy; topic; field(s); subject level(s). The sum of any combination of codes contained within these categories would then be capable of describing any one structural relationship in the data.

Having established that any one given situation of privacy thus deals with four
relational elements it then becomes necessary to, again, refer back to what a sub-theoretical notion is in order to determine the exact way these relational elements are to be framed by the SCA. The STN is defined as the “life of a concept”, involving how the ambiguity of a social phenomenon has been continuously refined to describe more perfected signifiers through the process of theorizing (Brown 2014). This means that the sub-theoretical properties of privacy, although related to the ways in which it is studied, are exclusive to the form the concept has taken and what has become a signifier for that form. In other words, of the four coded categories which describe all of privacy's various relationships in academic discourse only two, type and topic, represent the life of the concept. Both field and subject level are modifiers in the way privacy is discussed and/or studied but do not change the ways in which privacy manifests. As such it is then possible to establish types of privacy and topics (see Figures 6.5 and 6.6 below) as the organizing frameworks in which to present the actual structural content analysis.

<table>
<thead>
<tr>
<th>Figure 6.5: The Higher Elements of Privacy's Sub-Theoretical Notion (Types)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy as Relations</td>
</tr>
<tr>
<td>Privacy as Commodity</td>
</tr>
<tr>
<td>Privacy as Context</td>
</tr>
<tr>
<td>Privacy as Control</td>
</tr>
<tr>
<td>Privacy as Right</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Figure 6.6: The Lower Elements of Privacy's Sub-Theoretical Notion (Topics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
</tr>
<tr>
<td>Accuracy</td>
</tr>
<tr>
<td>Anonymity</td>
</tr>
<tr>
<td>Autonomy</td>
</tr>
<tr>
<td>Contracts</td>
</tr>
</tbody>
</table>

These two tables are entitled as “higher” and “lower” elements of privacy's sub-theoretical notion precisely because of their relationship with each other and manner in which the STN is defined. The title “higher element” is a reference to the distinction of each
contained code as either a primary form of privacy as a conception or its use as a top supra-heading element in the structural outlines of the texts. For the four codes pertaining to specific forms of privacy (communication, locational, medical and mobile) the contexts surrounding their discussion was unique enough that they could not be exclusively subsumed by the other codes. However, when any of these types of privacy are discussed they can be signified by any one of the topics in Figure 6.6. This is also the reason why the various codes for topics involving privacy have been regarded as “lower elements”; they are signifiers for a form of privacy, the perfected objects measured. In this respect, they were most commonly located as a sub-heading, under a type a privacy or at the same heading level in the structural outlines, denoting a strong relationship between the two.

The remaining two coded categories, field and subject level (see Figures 6.7 and 6.8 below), represent that last two components of privacy's relational complexities in academic discourse. These two categories mirror that which was discussed in the initial chapters of this study. However, while coding, additional levels of abstraction were delineated because it was determined that if combined the strengths of each one to describe a particular given contextual relationship would diminish.

<table>
<thead>
<tr>
<th>Figure 6.7: Identified Fields</th>
<th>Figure 6.8: Subject Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economics</td>
<td>Business</td>
</tr>
<tr>
<td>Economics – Marketing</td>
<td>Children</td>
</tr>
<tr>
<td>Legal</td>
<td>Individual</td>
</tr>
<tr>
<td>Social Sciences</td>
<td>Institutional</td>
</tr>
<tr>
<td>Social Sciences – Philosophical</td>
<td>National</td>
</tr>
<tr>
<td>Social Sciences – Political</td>
<td>Networks</td>
</tr>
<tr>
<td>Technical</td>
<td>Relational</td>
</tr>
</tbody>
</table>

A general approach to economics differed substantially from discussions of marketing, involving topics such as advertising in free-content services and data collection in unique contexts. While in the social sciences, approaches which engaged in matters specifically from a political or philosophical manner held what was judged to be significantly different assumptions and/or emphases. In Figure 6.8, on subject levels, it is recognized that these are not mutually exclusive items. However, in the structural elements analyzed within the generated outlines, each subject level listed inferred a unique degree of sociality/treatment.
Since each of these codes appeared to represent unique contextual relationships it was
determined that these seven codes were best kept distinct despite their overlap. It may be
good to note that “global” is not identified as a subject level itself despite having been
mentioned earlier. This is because it was subsumed exclusively by matters of “global”
information networks or a general discussion of institutions (governments). Any codes
presented in the earlier figures but not discussed within this section is because they will either
be discussed as part of the SCA in the following chapter or would have required substantial
portions of various structural outlines to serve as citational evidence thus over-emphasizing
auxiliary data.

Having been able to use the sampled texts to derive the order and a concise, yet
coherent, manner in which to discuss the totality of existing privacy-discourses it now
becomes possible to graph not only knowledge garnered from the analysis of the sampled
texts but additional resources, traditionally presented in the literature review, to produce the
SCA. The SCA in the following chapter will utilize a format based primarily on the
discussion of types of privacy as a way of finding patterns in existing discourses, shared
across topics and presented in unique ways according field and subject level.
Chapter 7- The Structural Elements Themselves As Things Stand

With a derived sampling of 4,486 structural elements, composing roughly 128 pages of outlined material, it was previously inefficient to provide all the necessary excerpts of the data to elaborate upon how each code within the final categories had been arrived at. While further methodological refinements may solve how to concisely present the process of coding, such as possibly designing a program to visually map the processes of dynamic programming, elaborations on the majority of the elements presented in each category is now possible in the literary presentation of materials. This should aid in providing justifications for their use, despite lacking transparency in the coding process earlier. This study must, once again, excuse any apparent logical leaps as a consequence of attempting to minimize both the length and complexities of this research material/process. Ultimately, as an exploratory attempt to produce a theoretical project on empirical grounds, certain aspects of this study can only realistically garner verification from the discovery of logical results.

7.1 Structuring the Structural Content Analysis

In a somewhat confusing capacity, the prior analysis was required to provide structure for the actual structural content analysis that follows. From the sample's analysis it was possible to derive the four relational categories involved in discussions of privacy and, through an understanding of what a sub-theoretical notion is, how strong of an emphasis should be placed in each category. A key realization was in recognizing the nature of the sub-theoretical notion to not be in the academic domains or subject levels involved. Although they are a part of the relational dynamics regarding how any one instance of privacy is discussed they are not central for this analysis of privacy's underlying logic. By this reasoning, when considering how to organize the SCA, both the involved fields and academic domains become secondary factors, only relevant to the discussion to the extent which they frame a conception and/or topic, but do not act as a molding force.

This simplified how to go about approaching the SCA. It is now understood that the key factors for elaboration do not the involve fields of study, despite being the main reason this study sought to find a theoretical foundation for privacy in the first place. Instead, the SCA must focus on the types of privacy in related discourses and the topics they address as the empirical representations of conceptual refinement and signifiers. By disregarding fields
and subject level it was possible to focus all acquired knowledge from constructing the prior analysis, as a methodological prerequisite for the SCA, towards discerning how each type of privacy related. This process was reiterative, shifting from reviewing the structural outlines and evaluating other sources gathered as the elements of a traditional literature review, to see how each type of privacy was discussed. The results of this process is the structuring of the SCA as follows, in preparation for the final critique in Chapter 8.

The remainder of this chapter is broken down into four sections, each detailing a perceived level of conceptual abstraction. In focusing on specific types of privacy discussed there is no direct orientation towards general, digital or physical privacy because these terms are containers for the employment of a conception in a specific manner. Clarity for these terms is to be established by the sub-theoretical notion extracted in the next chapter as a part of the results. Instead, each form of privacy is discussed as it appears in relation to specific conceptions. To help readers understand why this portion of the study turns away from the specific discussion of these particular terms, the SCA begins with an elaboration on the term “digital privacy” and its related variations found in current literature to point out its conceptual emptiness the STN aims to fill. Following this, in an attempt to avoid possible confusion later on, I classify four of the nine types of privacy found in the previous chapter to be sub-classes of privacy rather than independent conceptions. Then, in the most substantive portion of this chapter, I elaborate on the four major types of privacy as six related conceptualizations, presented as sequential conceptual developments, found in texts on privacy. A final section then provides an overview of topics (lower level elements of privacy as a STN) which were determined to be ubiquitous across conceptualizations but were contested as true signifiers for privacy.

Readers are reminded that a comprehensive and detailed overview of existing literature on privacy is beyond the scope of this study. Due to breadth and depth of possible related literature such an monograph would, at minimum, constitute a series of books in its own right. Instead this SCA-guided review will focus on providing a summary sufficient enough to demonstrate the overlap and interrelations amongst the multitude of approaches and elements involved. Furthermore, it was not intended for this discussion to be exhaustive within any categorization that follows. It is an accepted limitation that there will be specific theories, topics and applications which go unmentioned.
7.2 The Umbrella that is Privacy

The term “privacy” provides a great deal of flexibility in its conceptualization. Across literature this degree of abstraction appears to be intrinsic to privacy discourses. Studies may range from the narrow singular aspect of privacy to complex multi-dimensional notions. Rather than attempting to provide a clear definition for “privacy” itself many scholars have instead utilized a slew of delineated sub-terms. In effect, common terms such as “general privacy” become ambiguous and complex notions described by Daniel Solove as “a conceptual shorthand way to describe a cluster of problems that are not related by a common denominator or core element” (2008, 171-2). For example, Burgoon et al. (1989) when trying to encapsulate general privacy defined privacy as measures of physical, psychological, interactional and informational access to a person.

Yet, moving towards higher levels of abstraction, an analysis of privacy can become increasingly multi-dimensional by taking to account more than one signifier. In one such case, it was suggested that a general understanding of privacy could be achieved by breaking it down as a deliberation amongst three measurable forms: informational privacy, expressive privacy and accessibility (DeCew 1997). Lawrence Lessig, following a multi-factor approach, poses in his book Code 2.0 that any social system, including the role of privacy, has four regulators: market, law, social norms and technological architecture (1999). Interestingly, it is Lessig's attempt to not define privacy literally but as a sum of forces which reflects the four major academic domains of privacy discovered earlier: economics, law, social and technical sciences.

The largest problem faced as a researcher approaches the issue of privacy is its explicit ambiguity. Since there is no single form of privacy, rather, researchers have distinguished many different forms leading to a plethora of privacy-related terminology where each form can have reference to specific contexts, concepts or topics. This can become burdensome to readers at times since they share the same syntactic structure, “(x) privacy”, often with no conceptual distinctions. While this may not at first appear as an issue it emerges as one once the same terms begin to be used in different ways or in reference to different signifiers. As things stand, if “privacy” itself is to be considered an umbrella term then the issue is that its many variants have also come to represent smaller umbrella terms within the greater ambiguity of general privacy. Accepting that “privacy” itself holds no defined subject-matter, for clarity there must be an explicit elaboration as to what each “titled” form of
privacy refers to.

In the proceeding sections of this chapter numerous modifying terms will end up being used to describe particular versions of privacy and it can become confusing once these terms become compounded within a single argument while each refers to distinct elements not common across studies. While each term will be explained, the most important distinction to be made is that of why and how they are used. With the goals of this study to provide a theoretical grounding for privacy terms, thus finding the common denominator/core elements Daniel Solove proclaims to be missing, it is then important to preemptively establish why terms such as “digital privacy” and its variants, not just general privacy, are in fact conceptually empty umbrellas, only used in current research to describe contexts or specific topics.

Information privacy can be, and often is, treated synonymously with the terms “digital privacy” or “online privacy”. Defined most clearly, albeit openly, as “rules governing the collection and handling of personal data... [and] closely tied to [concepts such as the] security of private data and privacy of communications” (Bahdur et al. 2002, 45) information privacy has become a dominant term in modern research. Using this definition, information privacy refers to all related concepts and elements surrounding the treatment of information. It is then interesting to note its relative disposition for use in digitally oriented research despite not providing enough clarity define what “information” is. It is clear, often through its textual use, that information privacy refers not to information itself but to data, as a digital form of information. The main problem when using the term “information privacy” then is that information itself is not a concept restricted to data. Information can be verbal, written, descriptive or otherwise anything open to epistemological debate. So despite its prevalence in academia, information privacy is a term which will not be utilized in this study. Instead this paper employs the more specific, but still troublesome, term “digital privacy”.

Beyond being a reference to context, no adequate theoretical justification for the use of “digital privacy” over the term “privacy” was found in academic discourses. More notably, digital privacy was used to broadly address the technological circumstances attached to data and its potential uses. This distinction is more specific and, in effect, favored by this study over the greater conceptual issues brought up when using “information privacy”. However, the use of either term is predicated on the same grounds: they provide contrast to any other discourses where situations of privacy were studied without, in anticipation for, or
consideration of digital contexts. Thus academia is still faced with the issue that the only justification various terms is in establishing a point of reference between privacy in digital versus other contexts. Considering this notion, it can then be assumed that the prevalence of the term “digital privacy” and its variants (“online privacy”, “information privacy”, etc.) is due to their differentiation between two distinct notions: a historical ontology of privacy and the emergence of the digital, simply stated as physical versus digital context. Therefore, from here onwards, “digital privacy” will be used as a general term with no conceptual significance unless otherwise stated. As in the majority of other literatures, digital privacy remains an environmental descriptor of a situation without a true conceptual definition.

Regardless of the modifying term, it becomes clear that there is no explicit manner to define either privacy or, by association, any digital variation. Instead, it best acknowledged that the notion of privacy, in any context, is not an absolute term, rather, it requires the balancing of many interests, including the individual's and society at large (Culnan and Bies 2003). Conceptually, any form of privacy is a matter which resists a simple environmental classification. But despite this fact, modifying terms such as “digital”, “online” and “information” remain mundane forms for implying a distinction from the general term, still lacking theoretical substance without an explicit understanding of what distinguishes general privacy from its modified forms. By providing this substance through the sub-theoretical it is the hope of this paper that the trend of open-ended privacy terminology can be replaced by clear references to specific qualities.

7.3 Sub-Classes of Privacy

In a discussion of privacy many researchers rely upon additional sub-classes for clarity and distinction amongst various applications. These sub-classes of privacy follow the aforementioned trend of using modifiers to retain their own dimensions and/or specific qualifying contexts, rendering them unique but only to certain capacity within a given text. This makes any one sub-class of privacy inherently related to the major umbrella terms described previously but not bound to any specific one. With the emphasis on this analysis to work backwards from digital privacy, as the most refined form of privacy also giving rise to the conceptual distinction of physical privacy, the relationships sub-classes of privacy hold with larger conceptualizations must be clarified. In effect, although they are contained within discussions of digital privacy, they are not to be considered as elements of the sub-theoretical
notion because they lack their own conceptual properties. In this section I attempt to describe and differentiate these forms of privacy from the qualities of digital privacy terminology to show how they are related, but not intrinsic, to discussions of privacy online. The final result is that each sub-class of privacy is defined by the fact it only functions to describe particular contexts and/or conditions surrounding privacy concerns but make no conceptual contributions.

7.2.1 Communication Privacy
Communication privacy is generally a reference to the elements, controls and protections over personal communications (Acquisti et al. 2007; Belanger and Crossier 2011; Peteronio 2002). Clarke (1988) classified communication privacy as one of the four distinct dimensions of privacy besides privacy of person, personal behavior and personal data privacy. While this may seem to place communication privacy as one the core forms of general privacy it does not hold any conceptual significance. Today with most forms of communication having been digitized (e-mail, instant messages, texting, basic phone services, etc.), thus becoming a form of data, the majority of its applications are to digital interactions. However communications are not limited to digital, as with any written word or face-to-face interaction observed in the real world, the act of communicating can have either physical or digital dimensions. Communication privacy is therefore not a conceptual development in privacy-discourses but another modified term used to delineate specific subject-matter.

7.2.2 Locational & Mobile Privacy
Mobile and locational privacy are limited to discussions regarding the tracking of an individual's specific location at a given point in time. Location privacy can be defined as “the right of the users to decide how, when and for which purposes their location information could be released to other counterparts” (Acquisti et al. 2007, 313). Mobile privacy, in contrast, is set to a broader scale combining information on a person, location and activities into a complex set of relations (Trepte and Reinecke 2011, 192). A discussion of mobile privacy has grown from technological development, encompassing locational privacy, to describe cellular phones and the gathering of information from people in physical spaces through digital innovations. This includes the analysis of tracking technologies including but not limited to the use of Global Positioning Systems (GPS), reception tower
triangulation/ping'ing and radio-frequency identification (RFID) systems along with their
governing technical and organizational bodies. While GPS may be the most prevalent and
easily recognizable form of locational/mobile privacy related technologies discussions in
research move far beyond it.

Notable elements in discussions of this form of privacy include the combination of
these information types with other personal data to create real-time profiling and path
tracking. By integrating measures of location both these sub-classes of privacy are unique by
expressing a literal and direct tie between digital and physical forms of privacy. However,
these categorizations of privacy are primarily concerned with measures maintaining data
security, including encryption protocols and other privacy-preserving techniques. Overall,
they refer to systems of privacy, via specific contexts of data use and collection, rather than
conceptualizations of privacy itself. They are in fact, by definition, concerned with measuring
more fundamental conceptual elements of privacy including control, access and information
merging.

7.2.3 Medical Privacy
In respect to digital privacy, the sub-class of medical privacy contains no truly unique
element. It regards the restriction of access to health records and confidentiality. Medical
privacy is simply the extension of established ethical principles extended to either digital
conditions or its physical counterpart. Discussions of medical privacy express higher levels of
individual concerns over deeply sensitive and personal information. This is more a reflection
of cultural norms and its value within a society as a source of potential invasions of privacy
than a conceptual development. This specific area, with a higher level of general awareness
and existing legislation, thus garners specific attention from some researchers as an
application/example for other conditions and elements of privacy, such as third-party sharing.
Medical privacy does not, however, provide reference to anything more than specific subject-
matter and makes no attempt to define what privacy is.

7.2.4 Children's Privacy
Similar to medical privacy, children's privacy is primarily discussed as a special context
and/or example in broader privacy discourse. Discourse about children's privacy is one of
protection, security and control. Although not of any particular relevance to privacy as a
concept, the discussion of children's privacy is rather a reflection of existing social morals and ethics in a culture/family unit. By lacking autonomy, children symbolically represent the innocent and vulnerable thus are more readily subject to increased measurements of concern from parents/guardians (Desai et al. 2003, 20). This factor also amounts to social desires for specific legal regulations including the United States' Children's Online Privacy Protection Act (COPPA); one of the few pieces of American legislation that states concrete privacy boundaries by explicitly restricting the collection of data on any minors under the age of 18. Children's privacy is a lower sub-class of privacy defining only a specific demographic receiving special consideration/treatment but not altering the fundamental conception of privacy in any way. At best, children's privacy, much like the other sub-classes prior, provide a concise term to describe specific relationships amongst elements of privacy.

7.3 Major Conceptions of Privacy
Having eliminated four of the nine higher elements of privacy to be only significant codes for unique types of privacy but lacking conceptual components to make them theoretically significant to the sub-theoretical notion, the analysis now continues with the five remaining forms of privacy which directly addressed the question of defining what “privacy” is. From these five codes there were six major conceptualizations of privacy found in current literature, placing different emphases on specific relational elements. These conceptions were utilized across numerous studies as functional definitions of privacy capable of constraining a discussion and framing, in some manner, the interrelations amongst how topics (lower level elements) were addressed by field and subject level. Although related to a degree, each conception takes its own respective stance in regard to how privacy can be negotiated, maintained and altered by its signifiers. Their primary differences rest in exactly where the locus of privacy is and what constitutes an accurate epistemology when investigating particular behaviors and topics. The presentation of these concepts includes any connected theories but is important to note that this discussion is not on a theory of privacy. This study exclusively seeks to review the conceptions of privacy within digital contexts as a precondition to any theory of privacy, where theory itself is part of the empirical subject.
7.3.1 Privacy as Control

The conception of privacy as control defines privacy as a measure of the capability an individual has to restrict access to their personal information. Because the attributes of control can so easily be adapted to digital environments, particularly those of marketing/economics and information processing systems, it has emerged as one of the dominant conceptions in privacy research (Smith et al. 2011, 995). As will be detailed in the following pages, differences in how this conceptualization is utilized are found in how control is quantified and what degree of emphasis is placed on other relational factors. The importance of control in any conception of privacy will be carried through the remainder of the SCA as the most ambiguous defining element.

As a general approach, privacy as control can be traced back to the work of Alan F. Westin in the 1960's. Although Westin's contributions carried on until his death in 2013, his original book *Privacy and Freedom* succinctly phrased the loci of privacy as a means of control in the “claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (Westin 1967, 7). From this notion, Westin is accredited with transforming privacy debates and is widely regarded amongst privacy scholars as “the most important scholar of privacy since Louis Brandeis” for having recognized the emerging implications of technological development long before the Internet was ever introduced (Fox 2013). However, through his relation to Brandeis a key element of confusion does arise over the meaning of Westin's insights.

Although Alan Westin is accredited world-wide with being one of the most influential authors of modern times in the area of privacy research, his work has been adapted across countless studies beyond his initial notion of control, to be applied across numerous circumstances (Bamberger and Mulligan 2010; Belanger and Crossler 2011; Bennet 2008/2011; Sevignani 2013). As a lawyer and political scientist, his writing included aspects of sociology, psychology, law and economics. The problem thus becomes that Westin's work can be applied to nearly any discussion of privacy. In effect, as Westin continued refining his conception of privacy in later works to meet the desires of other academics his work also began to explicate the role of law to enforce means of control (Wessels 2012) and he began elaborating on privacy as a subset of states (Milberg et al. 1995; Smith et al. 2011). The issue Westin faced became how, when presented specific contexts, control is refined and operationalized; albeit by social norms, law, or economics. In response to the complexity of

62
privacy's many relational networks, Westin's initial conception of control became more refined but also more distant from its initial elegance as an ambiguous definition.

From Westin other conceptions of privacy as a form of control have developed. Sociologist Irwin Altman defined privacy, in an equally well-cited manner, as “the selective control of access to the self or to one's group” (1975, 24). In adding the element of “selective control” Altman builds from the influential work of Erving Goffman indirectly referencing systems of impression management and providing “control” a stronger interpersonal foundation. Similarly, Stephen Margulis, in an attempt to unify both Westin's and Altman's works, wrote “Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or minimize vulnerability” (2003, 249).

Margulis' conception of control as both interpersonal (“transactions”) and goal-oriented (“aim of which”) provides one of the most comprehensive definitions of privacy as control. Although not as prevalent in literature, by regaining a measure of variability, Margulis permits his definition to be considered a quality of privacy which is not exclusive of other notions. It can take into account a significantly larger portion of the relational codes arrived at earlier in Section 6.6. This is unlike the developments reflected in the majority of literature where control is considered exclusively to be the idea of one's ability to control (Smith et al. 2011). Defining privacy to exclusively be the ability to control is why it required refinement for specific contexts. Although mistakingly seeking further signifiers of control, notions of autonomy and vulnerability easily lent themselves as ways to operationalize control as key factor in shaping privacy (ibid., 995).

Issues in the conception of privacy as control remain situated in how it can account for the totality of privacy-related issues, specifically in digital contexts. One central concern is if control can situated as the most fundamental element in privacy, as posed by Westin's and Altman's definitions, or if control is more of a moderating factor as evident in Margulis' definition. While researchers across disciplines do utilize measures of control, Margulis' himself notes there are few theoretical attempts to clarify the nature of control in relation to privacy (2003). This study seeks to provide some clarity. With no clear answer if control is a moderating or fundamental factor shaping privacy, its role has been highlighted in the following alternative conceptions.
7.3.2 Privacy as a State

While ambiguity of Westin's writings on privacy is accredited as the foundation for conceptualizing privacy as a form of control, Westin's original book is also accredited more directly for establishing privacy as a state. In *Privacy and Freedom* (1967) Westin introduced four substates of privacy: anonymity, solitude, intimacy and the reserve. As further research progressed, his ideas evolved in proceeding scholarship. A distinction emerged surrounding control as a measurable variable or a completely subjective state of mind. Ferdinand Schoeman, mirroring elements of a concept of control, defined general privacy as “a state of limited access to a person” (1984, 3). Robert Laufer and Maxine Wolfe defined general privacy as a situational concept (a more technical variation of “state” allowing for constant change based on the social contexts of everyday life) split into three dimensions: self-ego, environmental and interpersonal (1977).

Although a unique conceptualization in its specifics, the notion of privacy as a state is not commonly reflected in the majority of literature. The unique quality of this conception is its focus on the subjective condition of being private. In doing so the subject matter for this conception is primarily located in an individual's perception of themselves in any given situation, a notion based entirely on subjective awareness. The research potential for is conception derives from its ability to consider a state of privacy as a sought-after-goal (i.e. a desire to be exist privately) and then evaluating this as a continuum (Smith et al. 2011, 995). Control, perceived or real, becomes a moderating factor to subjective awareness of existing in a state of privacy. In essence, control is measured as a feeling. Despite its unique qualities however, privacy as a state shares many of its premises with other conceptualizations. As a result, privacy as a state of mind is commonly subsumed within other derivative conceptions.

7.3.3 Privacy as a Right

Unlike the conception of privacy as control, when considering privacy to be right a more specific emphasis is placed on legality. The distinction of privacy as a right offers therefore lies directly in inferring what a “right” is. A right is an outright form of a legally enforced ability to control or the ability to claim control by invoking the authority and interpretation of law in a specific circumstance. The divergence from viewing privacy as control rather than a right is that former infers the state of having or not having control while the later explicitly involves claims of entitlement. A notion of privacy as a right thus views the role of
government and law to create and enforce a reasonable degree of privacy protection for society. In this way governments become treated as a primary antecedent to control.

Additionally, the right of privacy, as it pertains to law, must also require some notion of regulation. Under the conception of privacy as a right, researchers review established legal frameworks across all subject levels as the primary subject-matter for studying control. This places privacy as a right predominately within the legal and social domains in addition to acting as a regulating force on economics. Rights are social to the extent that a government functions to establish laws which promote societal growth and cooperation, a thought delineated from John Locke’s social contract theory. A right to privacy can become economic however when those said rights influence economic models, such as in the case of data-based subscription services. All of this can be seen by viewing the history of law as a history between public and private boundaries. Thus the study of privacy as a right becomes the subject matter of reviewing the implications of both digitally-specific and general privacy laws within a functional society.

Samuel Warren and Louis Brandeis's seminal article *The Right to Privacy* (1890), published in the Harvard Law Review, defined privacy as “the right to be left alone”. Since then, it has remained one of the most influential definitions of privacy in academic discourse, having been cited in nearly all investigated literature. This not without good reason. Their definition provided the origins for the development of a right to general privacy in the United States (Smith et al. 2011). Meanwhile, in some form or another, the same interpretation of a right to privacy has been recognized not only by the United Nations as a fundamental human right but also specifically stated in the Charter of Fundamental Rights of the European Union and countless other international treaties (Acquisti et al. 2007, ix).

Beyond its approachable and elegant phrasing, Warren and Brandeis also provided a much deeper understanding of what a functional definition of a right to privacy must contain in relation to its significance for individuals. While serving as a United States Justice thirty-eight years later, Brandeis, arguing for the expansion of US Constitutional interpretations to defend privacy, described the right to privacy as “...the most comprehensive of rights and the right most valued by civilized men” (Kuhn 2007, 7). Furthermore, Brandeis also had enough foresight to realize that any interpretations of privacy related law would have to be adaptable in accordance to “discovery and invention” not originally foreseen by the creators (ibid., 95). It is therefore clear that the most fundamental way of conceptualizing privacy as a right,
established by Warren and Brandeis, included emphasis not only on its importance for molding the social lives of individuals but would inevitably change over the course of technological developments.

7.3.3.1 Using Laws to Impose Privacy Rights
A great deal of research seeking an understanding of privacy through court cases and/or a historical ontology of privacy's legal developments can be found when viewing privacy as a right. This is, in part, due to the fact nearly every developed country in the world has enacted or is effected by some form of privacy legislation (Macella and Stucki 2003). Although specific digital or information privacy laws are far more sparse by comparison, the presence of any legislation involving privacy indicates privacy's direct relationship with various subject levels beyond the individual citizen. When functioning as a regulatory force, laws regarding privacy as a right, involve any scale of subject level from businesses to global relations. As such, the implications and issues surrounding the framing of privacy as a right arise.

Existing laws span a great variety of contexts and influence even more relational dynamics. In the United States, for example, legislation exists which impacts various subject levels in both positive and negative forms. The 1998 Children's Online Protection Act (COPPA) restricts the collection of personal information on children under the age of 13. This legislation not only acts as an enforcer of special protection for the privacy of children but impacts various business models and the economics of supplying free-content online through the commodification of user information (Henderson 2006). The Gramm-Leach-Bliley Act (GLB) of 1999 regulates the uses/sharing of financial data by expanding the legal capacity for sharing/merging of banking, insurance and securities company databanks. While designed to aid the financial system this also has presented issues surrounding the types of data gathered on individuals and the exact ways in which it is used (ibid.). Finally, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, addressing electronic health care transactions, provided an enforced regulatory framework and standards which required providers to allow individuals to see their own files (Henderson 2006), a right not often granted to individuals over the wills of businesses nor broadly available outside of medical records. Each piece of legislation brushes upon different notions of privacy and addresses a wide range of very specific relational dynamics.
Privacy-related laws however are not constrained to the protection or reduction of rights *per se*. Another aspect of a right to privacy involves criminal law by determining what can be considered private property or an invasion of privacy. Within the contexts of a digital environment this involves what is to be considered a cybercrime and it is in this sector of law, specifically, where technological development often outpaces the legal. This disjuncture appears predominately in notions of security and can impose privacy risks in two major ways: (1) a lack of specific or applicable criminal law and (2) sweeping privacy-invasive legislation. While the former is perhaps more common the later is of particular concern for the general public. One such example is the signing of the United State's Patriot Act in 2001 which permitted sweeping surveillance and tracking of phone/internet activities from data gathered both domestically and internationally (Bahadur et al. 2002, 125-30). However, the control of information practices and security standards by law is not exclusively restricted to a single nation. Quite often certain policies can not only cross national boarders directly but can also have transnational impacts.

The European Union has passed a great deal of legislation which covers these areas. In the EU Data Protection Directive of 1995 broad scale regulatory standards were created for the processing of personal data within EU member nations. Included under this legislation are specifications that user consent must be “freely given, specific and informed” (Article 2), no data shall be processed “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … data concerning health or sex life” (Article 8), citizens are protected from decisions “based solely on automated processing of data intended to evaluate certain personal aspects” (Article 15), and that member states must establish appropriate sanctions to deal with privacy infringements (Article 28). Covering topics in privacy such as notice, choice, transfer, access, security, accountability and data integrity, the EU Data Directive is regarded as the most comprehensive information privacy legislation to date (O'Connor 2007).

While the European Data Directive undoubtedly establishes a great deal of positive privacy rights for member-state citizens it also had profound global impacts. Article 25 has a substantially larger scope by requiring that any personal information being moved outside of the European Union may only be sent to countries which can guarantee an adequate level of protection. Although exactly what constitutes “adequate” is unclear, this broadly influences how data is treated around the world. In the United States for example, which is the primary
location for many of the world's most popular online services (Facebook, Google, Twitter, etc.), the Safe Harbor certification program was established by the U.S. Department of Commerce in consultation with the European Commission to streamline a self-certification process for the transfer of personal information (Merkow and Breithaupt 2002). From this, numerous voluntary and self-regulatory “privacy seal” certification programs developed, including widely recognized TRUSTe seal, which supply websites with visible markers indicating they meet Safe Harbor principles and/or other “seal” specific standards (Bahdur et al. 2002, 62-63; 82-84).

The EU Data Directive and subsequent seal programs reflect the many forms privacy laws can take as well as their implications. What Safe Harbor and other certifications uniquely represent however is a shift from mandatory (hard) regulation towards voluntary (soft) regulation. Soft regulation presents a stronger social and economic emphasis in law because they are voluntary actions taken by companies. Specifically, what changes for the individual under the guidance of soft regulations is the potential of redress available should a company fail to meet a representative standard. While hard regulations are enforced through governments, soft regulation is self-compliant or, in the case of seals, monitored by a third party. Should a company displaying a seal be found violate its principles redress in this case ultimately comes in the form of revoking the right to display that specific seal. In comparison to the many possible punitive actions which can be sought by governments and individuals through regulatory law, the punitive actions possible through self-relegation are far weaker. In addition, regulatory organizations such as TRUSTe often have limited resources thus impacting the efficiency of any compliance monitoring.

7.3.3.2 Privacy Under the Laws of Property
In another direction, some scholars who argue a right to privacy often draw upon an implicit relationship between dominant privacy notions and the legal notion of private property. By relating privacy to a form of property it develops stronger forms of personal control by building from the established measure of non-consensual access prohibited by most forms of property law (Sevignani 2013). To this degree, it then becomes vital to understand how privacy may be regarded as a reasonable extension of property law by governments.

From its very origins the term “property” establishes an intimate relationship between the social and legal domains. The modern term “property” derives from the Latin proprietas,
itself, derived from the term *proprius*, an adjective, applicable to physical things or qualities meaning “to own” or “peculiar” as opposed to *communis*, “common” or “anothers” (Reed 2004). Property is commonly understood to be composed of “what one owns” (ibid.). However, this definition falls short of elaborating on what “ownership” actually is. Within the social sciences, property is most commonly affiliated with social relationships of power. Within jurisprudence the two most commonly held stances are those of the Lockean and Blackstonian conceptions. These conceptions stand in contrast of each other on the pivotal theoretical issue of if property is rooted in isolation as a descriptive and normative baseline, Blackstonian, or requires the presence of society to generate the individual nature of property, Lockean (Davidson and Dyal-Chand 2010).

William Blackstone, an 18th century English professor of law, developed one of the fundamental definitions of property as “the sole and despotick dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe” (1765, 2). Blackstone's definition became the foundation for developing property in common law as the “right to say no”, a negative right of exclusion (Schmidtz 2010). From this a second, more modernized, notion of property has also evolved: the bundle of sticks metaphor. Moving beyond a single definition in order to encapsulate varying perspectives, the bundle of sticks metaphor describes property as a *set of rights*, including qualities such as the ability to sell, lend, bequeath, use as collateral or even destroy (Reed 2004).

The properties assumed under the consideration of privacy as a form of property are pivotal in establishing a new emphasis on the different domains involved in the abstract nature of digital privacy as a matter of personal information. Privacy, when extended to property rights, places far more emphasis on not just general measures of individual control over personal information but also on the knowledge and conditions of use permitted. As property, privacy finds itself situated in the negotiation of uses otherwise regulated via the extension of property law. The right of negotiation, as an added layer of complexity, thus brings additional issues of consent and personal autonomy to light (Reed 2004). The role of social and economic factors are heightened. From this standpoint, although still framed by law, a new conception of privacy arises with its primary loci of attention on economics, the conception of privacy as a commodity. In this approach to privacy it is fair to then reconsider the notion of a general right to privacy towards a right to *some* privacy— moderated by
necessity of economics, the regulatory force of law and the struggle to keep private property protected as it takes on new forms no longer directly protected by the law (Bahdur et al. 2002).

In summary, when privacy is defined as a right it inherently emphasizes legal systems as a molding force for implicit and explicit forms of control. The study of privacy as right however is left with subject-matter composed of the legislation itself and an open-ended interpretation all of the relational dynamics entailed. Thus the study of privacy as defined by law becomes a delicate matter of studying the balance amongst various interests. While undoubtedly capable of addressing every matter of privacy to some respect, this conceptualization has done little to describe what the intricate and complex matters of privacy are or why they exist besides providing a frame in which to view these issues. Law, as the embodiment of a right, does not hold a strong theoretical standing for explaining privacy as much as it does explain how power is exercised in issues of privacy. Then accepting its own struggles to regulate privacy as technological development outpaces legal clarification. Rather than provide a straight-forward definition of privacy this conceptualization offers a continual platform for debate with the extension of property law to digital information at its doorstep.

7.3.4 Privacy as a Commodity

As the conception of privacy as a right faded into the debate over an extension of property laws it began to encroach upon the central elements covering the conception of privacy as a commodity. In general, the commodified perspective of privacy is rooted in the economic factors of everyday life resulting from technological development. It has emerged as a dominant way of viewing not general privacy but the particular conditions surrounding digital privacy. Due to the development of information-based societies and the prevalence of free-content digital services, combined with rising public concerns over digital privacy, this area of research, described in the opening chapters of this paper, dominate current privacy-discourses.

A desire to understand digital privacy created the privacy as a commodity conceptualization. Because digital privacy is a pervasive element of modern life, found anywhere technology has had influence, it is an area that involves all domains of research and a broad spectrum of topics. The apparent bias presented in the length of this section is a direct
result of this complexity. Furthermore, since it is the one conception of privacy that is exclusive to digital contexts, the conception of privacy as a commodity is also the most critical point of this study to establish not just what privacy's latest conceptual refinement is but also detail what composes its justifications for being segmented from other forms. It is the most important section of this study in order to not only discover what the sub-theoretical notion of privacy is but to then, later, derive what about privacy's STN has been altered so dramatically as to explain its conceptual distinction. Therefore, it is the goal of this section, not to overwhelm but, to highlight the many facets of privacy research contained within this conceptualization that one must consider while contemplating its relation to other discussions of privacy.

7.3.4.1 Economic Properties of Information: Marxist Perspective

In order for information to have any economic substance they must contain value in some form. Karl Marx, in his critique of capitalism, provides a framework for recognizing how this is possible. Elaborating that any given commodity, to be classified as such, must have a use value (why someone wants it) and exchange value (a means to buy in an exchange process) the source of value is found in markets. His fundamental principle includes that, through a division of labor, the laborer himself is the fundamental source of all profits through the production of surplus value, in form of their labor power, exceeding what is initially supplied by the investor/capitalist. As a basic law in Marx's critique, the mass of surplus value (total surplus value produced) is gauged by the quantity of workers and how much surplus can extracted from each (Marx 1867).

While remaining an active debate, the acknowledgment of information becoming a central form of value in global economics is widely recognized in the many ways scholars have attempted to classify and explain modern societies. Daniel Bell's (1973) knowledge society functions as a classification determined by the rise of knowledge based labor in tandem with a decrease in manual labor. In Manuel Castells' notion of a networked society economies are defined by the interrelation between modes of production and development, then identifying capitalism and informationalism as these elements in current developed societies (2000, 14). By the words of Hardt and Negri, contemporary societies are defined by the production of immaterial labor which “creates immaterial products, such as knowledge, information, communication, a relationship, or an emotional response” (Hardt and Negri
The relevance of these principles can be applied to a digital conceptualization of privacy because they establish how current technological developments have altered capitalist models to seek value in information at an unprecedented scale.

When access to online services is free, as described in Chapter 3, the source of value must be considered. By the very nature of capitalism an economic model focused on offering a product for free cannot generate profit. It is fair to assume then that the service itself is not the product being offered. The new location for profit in free-content services thus rests in the consumer/user of the service. This model of production through consumption was coined by Alvin Toffler (1980) as the “prosumer”. However, within the contexts of digital media, specifically social media, it is important to note that prosumption is primarily a means for outsourcing labor without payment (Fuchs 2011, 297). As internet consumers are always in a state of activity when online they are always acting as prosumers resulting in a transformation of the audience commodity into a prosumer commodity (ibid.). The development of the prosumer/produsage class of labor is hence not a democratizing force but a signifier of the complete commodification of human creativity (Fuchs 2010, 192). The conclusion reached by these arguments is one of startling significance: as capitalist models and global economics have moved from material based economics to the immaterial/information based they have simultaneously created ways to transform everyday life into value-producing prosumption via commodification of our actions.

7.3.4.2 Privacy with the Values of Property
In contrast to the prior section on privacy as right, from the economist’s standpoint, privacy is not an absolute right. Instead, such treatment would actually be regarded to have negative impacts on the health of information markets (Bennett 1995). In the economist's view, privacy is a matter subject to consumer rationality and autonomy by employing economic principles of cost-benefit, trade-off or risk assessment analysis. It is from this treatment of privacy that the conception of privacy as a commodity arose (Campbell and Carlson 2002).

Discussed earlier in sections 7.3.3.2 Privacy Under the Laws of Property and 7.3.4.1 Economic Properties of Information: Marxist Perspective, privacy is subsumed under the laws which apply to property once it has been given value as a commodity. It then becomes necessary to explore the assumed set of rights attached to forms of property. On a basic level, this means not only having the right to control access but the right to negotiate it as well.
Privacy then, by this logic, is defined, in part, by the ability to negotiate its boundaries, defining when and how information can be collected/used. From this there is a significant reconceptualization of privacy away from the notion of a right and towards a commodity which can be exchanged for perceived benefits (Campbell and Carlson 2002). In this manner a complex relationship is established across legal, social and economic spheres: law moderates a market's ability to negotiate the privacy of individuals by redefining measures of control over valuable information. Studying digital privacy is then a multilayered process, with elements stretching across each academic domain yet also simultaneously molded by the technical architecture of the internet. These factors are implicit to the privacy conundrum caused by e-commerce first described in Chapter 3.

7.3.4.3 Impact of Data-Based Subscriptions

End User License Agreements, also known as EULAs, “Terms of Use” (TOU) or “Terms of Service” (TOS), are formal contacts which designate the exact terms and conditions a user is subjected to and must be agreed upon before use of a digital service or software. The Terms of Service and/or Terms of Use utilized in e-commerce are commonly referred to in legal studies as 'adhesion contracts'. These contracts are prepared by one party, in this application the online service, and signed by another party, users, who must adhere to terms as written while having almost no option to alter any terms that are unilaterally set (Garner and Black 2006, 143). The extent to which adhesion contracts have managed to perfuse daily life is immense and often goes unnoticed. As stated by Peter Linzer:

“Adhesion contracts have grown in importance with the rise of e-commerce and changes in mass marketing. In the old days many transactions were really barters. You bought a book and handed cash to the clerk. Any problems were controlled by implied terms imposed first by the common law or merchant law and later by the Uniform Sales Act or the U.C.C. Now you go online to Amazon or BarnesandNoble.com and at some point click on an overriding agreement that is supposed to govern your transactions, and that changes many of the default rules. You pay by credit card, subject to a long, printed agreement that, according to its terms, can be changed unilaterally by the card issuer. You download software connected with the book and click to "accept" the EULA (often expanding the manufacturer's property interest under the copyright laws) as part of the installation. Et cetera, et cetera.” (2008, 206)

The prevalence of adhesion contracts brings into question the roles and relations between law, economics and society for privacy. They are the legal means of defining how data will be controlled and has affected anyone using a digital technology. It becomes reasonable to presume that digital adhesion contracts may have shifted from mere forms of private
contracting towards effective measures of public policy of which the public itself has no say or influence. Phrased by Christian Fuchs,

“Users have hardly any choice not to agree; if they want to interact with others and make use of the technical advantages web 2.0 poses, they have to agree to these terms. Privacy statements are totalitarian mechanisms that are necessarily not democratically controlled by the users, but under the control of corporations” (2011, 303)

From the standpoint of privacy as a commodity, law and markets prevail. These two forces act in tandem to create the privacy concerns reflected and studied in digital privacy literature. If information has value and users have become prosumers, constituting the complete commodification of their activities, then it is through online services and specifically e-commerce models that this shift has developed so dramatically.

By looking at the relational shift between digital economies and users an understanding of the failures of legal fields can be placed into focus. Legislation and e-commerce can be viewed as opposing or supporting forces. From a political-economic standpoint the fundamental place of law is to moderate the needs of society but, as some researchers adamantly argue, currently the needs/desires of people are being suppressed by the economic weight of privacy commodification. However, without first addressing consumers and their position within current economics no efficient conclusions can be drawn. Theorist Michael Raphael highlighted that there has been a fundamental shift in the way commercial interactions takes place between services and users, uniquely grounded in the commodification of information. This shift (detailed in Table 7.1 on the following page) elaborates on how the concept of data-based subscriptions can rephrase the issues surrounding information commodification.

From Raphael's work it becomes clear that under adherence contracts a new economic model is dominating e-commerce which places the relationship between user and service into new terms not often recognized by other researchers. Consistent with notions of commodification and prosumtion, users are placed into a relationship with a service which continuously seeks find and extract value from user generated data. This relational shift alters how fields should approach digital privacy and frame privacy as a commodity. If contracts are central to how information is commodified then contracts should become one of the primary subject-matters for privacy as a commodity. And, in fact, a large portion of research does acknowledge this while seeking out how to evaluate contracts in a meaningful way. However, as will be explained, the way this is commonly accomplished fails to recognize
limitations of the privacy as a commodity conception.

<table>
<thead>
<tr>
<th>Table 7.1: Types of E-Commerce</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table 7.1: Types of E-Commerce</strong></td>
</tr>
<tr>
<td><strong>Traditional Commerce</strong></td>
</tr>
<tr>
<td><strong>Advertised Consideration:</strong></td>
</tr>
<tr>
<td><strong>Means of Contract:</strong></td>
</tr>
<tr>
<td><strong>Means of Consideration:</strong></td>
</tr>
<tr>
<td><strong>Delivery:</strong></td>
</tr>
<tr>
<td><strong>Transaction:</strong></td>
</tr>
<tr>
<td><strong>Nature of Transaction:</strong></td>
</tr>
</tbody>
</table>

Taken from: Raphael, Michael. 2013. "Contracting the Internet- Governance or Commerce"

7.3.4.4 Contracting Privacy in the Lens of Autonomy
Privacy-related literature has addressed adhesion contracts in many ways but often with particular focus on Privacy Policies (PPs), a sub-form of Terms of Service/Terms of Use usually linked or refereed to in the primary terms, as a document detailing matters related to privacy that service is required to disclose. Using privacy policies as a primary source, economists, legal scholars and social scientists alike have attempted their evaluation under different criterium to address their effectiveness. Effectiveness, in most cases, is correlated to various degrees of actual use and reader comprehension by visitors. A majority of research has thus sought evaluate the effectiveness of privacy policies through measures including: accessibility; readability; regulation; consent models; user access to information; servicer security measures to protect information; arbitration; how information is collected, shared and used; storage and retention rates; and information sharing amongst services and “third
party-services” (Anton et al. 2004; Bonneau and Preibusch 2009; Culnan and Bies 2003; Desai et al. 2003; Earp et al. 2005; Jensen and Potts 2004; Liu and Arnett 2002; McDonald et al. 2009; Pollach 2007).

In a survey conducted by the Progress and Freedom Foundation in 2002 an estimated 77% of websites employed privacy policies of some manner while 91% of American commercial websites collected personal information and some 90% collected personally identifying information (Jensen and Potts 2004). This demonstrated that, in the not too distant past, despite commodifying user information for profit, a degree of online services supplied users no opportunity to even read the terms they had agreed to regarding privacy. However, given the increasing rates of privacy concerns reported by internet users, a fundamental issue preceding any notion of privacy policy research is the question if any adhesion contracts (terms and privacy polices) are actually read when present. Through survey research this question has been thoroughly explored and the answer is simply no. Most consumers seldom read privacy policies when given the chance or asked to (Graber et al. 2002; Turow 2003; Vila et al. 2003). With empirically verified reasons including general issues regarding length and the difficulty of understanding the legal phrasings used (Pollach 2007). The rationality behind this is simple: the calculated costs of reading privacy policies for the average American, visiting only 119 websites per year, are in the order of $781 billion dollars (McDonald and Cranor 2008).

This is a critical point not acknowledged by many authors who decide to study the format and various elements of privacy policies as reliable measures of the status of user privacy. The value of knowledge and insights into how and what is contained within the PPs is limited in their applications until the reasoning behind why privacy policies are not being read can be accurately pinned down. Measures of readability, length and phrasing are indeed issues. But they are far lower in the orders of abstraction within their relation to digital privacy because they end up relying upon so many other notions/conditions. If privacy can be considered subjective as a state, which was not refuted by any of these studies, then a fundamental aspect of privacy has been denied its weight when attempting to describe privacy as a whole, despite any clean empirical measures gained from the study of privacy policies.
7.3.4.5 Beneath the Veil of E-Commerce

Moving away from privacy policy research and the significant role of law, the next matter of concern is recognizing the literal actions taking place in data-based subscription services to commodify user data and the ways this relates to user privacy. This area of relations focuses primarily on the economics of selling digital advertisements and the technology behind the gathering/use of user information. However, there is an dangerously low level of knowledge about what actually occurs within the background of the internet, even amongst privacy researchers and particularly amongst those without a technical background. This lack of adequate knowledge about the internet's inner-workings extends beyond just the consumer and well past the human sciences as iterated by prominent privacy scholar Helen Nissenbaum, “[t]he technical and institutional story is so complicated that probably only a handful of deep experts would be able to piece together a full account; I would hazard that most of the website owners who contract with ad networks providing targeted advertising services are not among such experts” (2011, 35). Countless technical elements including server networks, scripting protocol, geo-tagging, external and internal resource requests, etc. build layers upon layers of technical haphazards to produce to so-called inner-workings of the internet. This brings into question how the technical architecture of the internet and specifically, e-commerce, fundamentally influence and construct how digital privacy can be affected/changed. In addition, this allows one to question the practicality of studies advocating for greater user autonomy. If researchers across disciplinary fields cannot accurately pin-down what happens behind the veil of data-based subscriptions it is no longer a reasonable stance to assume consumers should take on this burden.

In online advertising there is a system of ad-networks, companies that are designed purely for the collection and utilization of information gathered from users, known individually as data-brokers, to ensure that targeted-advertisements and marketing profiles of individuals are accurate. These companies work in murky waters navigating the legal and social spheres of digital privacy. Ad-networks often function as the third-parties mentioned in privacy policies with no explicit mention of how their relationship is defined. They are the invisible markets connecting multiple websites which have collected information or have advertising space to sell while simultaneously acting as buyers and gatherers of information themselves.

There are a variety of manners in which ad-networks can collect and use information.
Three general forms are: (1) the collection of personal data that is then anonymized and aggregated to sell to other parties and/or use themselves; (2) collection of personal data that remains identifiable only within the company but provides the opportunity to sell targeted-marketing under a specific range of cataloged traits; and (3) the collection of personal information with the intention of selling to anyone with an interest and money without taking steps towards anonymization (Christiansen 2011). Nevertheless it is not just ad-networks which gather information nor are all of their methods of data collection composed from their own surveillance methodologies.

Clickstream data is transmitted openly as a required element of the internet's infrastructure, functioning as the “to” and “from” data-routing element. However, clickstream data can also include information like key words or search terms or items in a shopping cart (Dana and Gandy 2004). The storage and retention of clickstream data by visited websites comprise what is commonly referred to as web logs or user logs (Macrella and Stucki 2003, 27). These logs can pose particularly distressing privacy concerns on services such as Google.com and other search engines where they include all data related to what a particular person has been looking up and what links were clicked. The aggregation and use of such data allows for companies to conduct a path analysis of where a user has gone when surfing the web. In situations such as the PRISM program described in Chapter 3, router manufacturers and internet service providers (ISPs) must naturally receive and record this data however this enables any entity with the authority or capability to access this data a slew of potentially sensitive information.

Yet clickstreams are not the only way to track user activity across multiple websites, another method is element placing such as Google's “+1”, Facebook's share/like buttons, Twitter's “Tweet this” buttons, etc. which all add tracking elements to the pages they are added. It does not require actively using these elements but their mere presence on a webpage which enables the companies which supplied them to track visitors. In this way, these companies can have elements which track users implicitly across numerous pages they do not own or operate. One such study found that Google had its presence on 80% of sampled websites while Facebook had an 85% rate of presence in the top 10% of popular websites world-wide (Gill et al. 2013). While these figures provide a startling insight to the possible amount of information some of the most successful web-services can gather perhaps the most well known, thus studied, tracking elements are cookies and web bugs.
Cookies are composed of a short string of text which is created on a computer's hard drive when accessing any website using cookie technology. Any active element linked to a particular web-service on a website can place a “third-party cookie”; meaning every button, uploaded font, image or graphic element can host scripts which place cookies on a visitor's computer. When cookies are utilized by ad-networks they become capable of tracking users across any website which serve ads that they are in contract with. In addition, through a process called “cookie-syncing” is has been discovered that a tracking service, such as those in an ad-network, can identify cookies holding collected data on servers outside their own and send a request to then sync their databases without any activity on the user-end (Englehardt 2014). This is possible because cookies store a unique identification number, expiration date, IP (Internet Protocol) address of the user, basic web browser data and the domain which established it (Macrella and Stucki 2003, 27). By using IP addresses ad-networks become capable of selling and buying other aggregator's tracking data. Likewise, web bugs hold the same information as cookies but are virtually undetectable as invisible elements 1x1 pixel in size. They cannot be prevented by users and, with a prevalence equal to cookies, are capable of tracking users in spaces where cookies are not, thus supplementing cookie tracking. When the totality of web-tracking data is combined and then processed with aggregate information about the types of services visited, including referring sites, a rather detailed picture of user behaviors can be created.

However, the actual processes and extent of data broker databases are kept far from the public or scholarly eye. Scott Howe, the CEO of Acxiom, one of the major US-based data brokerages, gave a chilling remark in an interview about the general attitude his industry has towards inquiries: “…we haven't shown people what we actually do when we cleanse the information and build models on top of things... [we're] an industry that's been cloaked in secrecy for 30, 40 years…” but then elaborates why, in their view, privacy is of little concern “5 to 10% of the people were going to be uncomfortable with any kind of information ever being shared about them. In contrast, 10 to 15% of the American population absolutely doesn't care” (Wack 2013). Yet what Mr. Howe has failed to account for is what existing privacy research has already established. Once consumers do become more aware of the degree, methods and analytical processes of data commodification there are significant rates of consumers changing their views towards online advertising as an invasion of their privacy (Sevignani 2013, 736). In this sense, systems of e-commerce face a tension between being
informative and consumers’ distaste for data use (Tucker 2012). This is held in particular regard for specific types of data such as healthcare, children-oriented and financial data where more specific targeting effectiveness provokes stronger privacy-sensitive reactions (ibid.).

7.3.4.6 Privacy Concerns
The progression of privacy as commodity thus far has followed a basic progression: its establishment as a form of property in information capitalism, spurred by the development of data-based subscription services, then enforced as contracted privacy and issues surrounding subsequent forms of data collection used for commodification. These stages have demonstrated systems of relations amongst privacy as a commodity over every coded field and numerous topics which have intrinsically brought about specific privacy concerns. This sub-section details the remaining topics which have specific relevance to user privacy concerns.

Designing default options for privacy is one such element commonly studied as a signifier of overall digital privacy standards. Specifically, these studies focus on opt-in versus opt-out defaults across web-services. Opt-in versus opt-out options describe the passive condition of either agreeing to certain practice, typically forms of data gathering and targeting, or not. As a default, despite the fact they represent a choice, one must always be active. Setting this default is the choice a service makes for the user unless it is changed. While some author's choose to argue that changing the majority of defaults to opt-in would dramatically improve the general state of online privacy by reducing the amount of things consumers are implicitly agreeing to, thus providing choice as a measure of control, this is a one-dimensional viewpoint. There are explicit and often disregarded reasons this does not happen from an economic standpoint. Opt-in solutions reduce the number of potential users that would otherwise be subject to advertising and data-surveillance (Fuchs 2011). This may enhance digital privacy standards for users but it would also undermine the economic principles of data-based subscriptions, possibly jeopardizing the validity of such models.

Another factor related to concerns over digital privacy is data-based discrimination, one of the largest intentional and unintentional forms of potential privacy harms online. Data-profiles are typically incomplete to some regard despite attempts to produce larger datasets. Some advertisers, consciously aware of a higher level of potential error in their
categorizations of profiles, use sweeping methods of targeting regardless. One researcher relates these actions to the Pareto Principle, 80% of profits come from 20% of a companies consumer base, where a service's most valuable customers are more likely to have been targeted correctly thus the successful personalization of ads and communications for these customers constitutes a profitable action even if the majority are wrong (Danna and Gandy 2004). Furthermore, this principle can be applied in the inverse by utilizing group/categorization based price discrimination to 'wepline' or exclude certain classes of consumers from a marketplace (ibid., 382).

Yet, one of the greatest issues surrounding digital privacy is the privacy paradox. The privacy paradox addresses studies which have shown that regardless of raised concerns and/or higher levels of technical knowledge consumers are still readily willing to provide personal information in situations contradicting their concerns (Acquisti and Grossklags 2005). One such study found that even under controlled settings where users were given a small (one euro) discount for providing more private information when shopping versus the same site with no personal information requested at regular price 93% the sample chose the lower price despite 77% stating they had high levels of concern for their personal privacy (Beresford et al. 2012). Then, more surprisingly, when prices were equalized over half participants still chose to buy from the aggressive site (ibid.).

However, this could also be an issue regarding what “privacy concerns” actually are. Studies have shown that average lay-person will fail to recognize privacy under the same definition as the researcher (Paine et al. 2007). The privacy paradox thus threatens any measure of privacy calculus (the balancing of risks/costs and benefits) as well as measures of trust which a large variety of studies have tried to operationalize (Smith et al. 2011, 10). Clearly, the statements many individuals make regarding their privacy concerns and related intentions may not reflect actual behaviors. This may very well has serious implications for, if not invalidate, a great deal of premises studies involving economically based logics of risk-benefit analysis and rationality utilize, in addition to questioning the general notion of using privacy concerns as informative of what practices are actually most harmful to society.

7.3.4.7 Commodity Based Theories
Direct comprehensive theories on privacy are extremely hard to find, most likely due to the conceptual ambiguities this project is based on. Over the course of this study only one
instance of a true theory on privacy was discovered. The majority of research seeks to explain privacy only through its signifiers which appear in specific contexts. A theory of privacy actually expands a conceptualization of privacy to a framework capable of being tested to explain all situations of privacy.

Justice Theory frames online privacy as a contrast between a right to privacy and, under commodification, that consumers are rational actors. It is a framework consisting of two theoretical notions: procedural and distributive justice. Procedural justice is focused on recognizing the individual and social elements related to how consumers feel about the perceived fairness of business practices in relation to their policies or rules. Distributive justice focuses more on the material well-being of individuals by addressing the perceived fairness of outcomes and gain allocation. In this sense, procedural justice is primarily concerned with how consumers feel respected and valued while distributive justice centers on if the outcomes from their relation are distributed appropriately (Ashworth and Free 2006, 114).

Justice Theory uses these notions of distributive and procedural justice to evaluate the conditions and reasons for privacy concerns. However, it arrives at a point of theoretical concern precisely because it relies upon the assumptions that consumers believe they have ownership of their personal information and understand the full extent of the exchange taking place (Ashworth and Free 2006; Turow 2003). Previously discussed studies have shown that these presumptions are flawed. Justice Theory compounds multiple subjective signifiers, based on individual perceptions, and claims that individuals are rational actors by having a realistic understanding of what is being agreed to. The entire premise of this study and, particularly, of this section have been to demonstrate the complexity of measuring privacy's signifiers and a lack of understanding by researchers, let alone the average lay-person. Then, because Justice Theory uses a foundation based in other concepts like rationality, fairness and exchange to account for the idea of privacy as a commodity it demonstrates Brown's failure to be progressive by not recognizing the fact that it makes contested notions unquestionable (2014). It is a theory built from the continual conceptual refinements of privacy and thus ignores its own sub-theoretical obligation to the actual conditions of life which brought about privacy in the first place by explaining these conditions to be known derivatives of privacy. All-in-all, Justice Theory demonstrates why the sub-theoretical notion of privacy is necessary to provide a true theoretical grounding for the production of future theoretical developments.
7.3.4.8 Summary

When viewing privacy as a commodity what ultimately must be balanced are the socially grounded concerns of individuals, legal frameworks and the assured stability of an economic system based in extracting value from personal information. However, a predominant amount of this research falls victim to unconscious value-laden assumptions about what elements of privacy are to be emphasized (Smith et al. 2011). The conceptualization of privacy as a commodity has provided the qualities, topics and relationships which aid in understanding why digital privacy has been viewed as a unique form of privacy by researchers. It exists within a technological infrastructure which integrates matters of the social, legal and economic at nearly every level. Effective resolution of digital privacy matters requires a delicate balance of the entire system of relationships privacy has in addition to an increased level of technical comprehension surrounding the collection/use of data.

In essence, the privacy as a commodity perspective demonstrates a reconceptualization of privacy away from elicit rights and towards the standpoint that privacy can be exchanged for benefits. Out of this process of exchange the relationship privacy holds with the power of law is also changed. This relationship becomes one more centralized on economic concerns than the protection or expansion of personal rights to privacy. For example, recall the EU Data Protection Directive of 1995 which established progressive, new, rights for digital privacy within the European Union. It becomes interesting to note that in the European Commission's 2010 report, “data protection” was not classified under “Strengthening individuals' rights” but rather apart of “Enhancing the internal market dimension” (Hornung 2013, 187). Put succinctly, “Under the commodity view, privacy is still an individual and societal value, but it is not absolute, as it can be assigned an economic value and be considered in a cost–benefit calculation at both individual and societal levels” (Smith et al. 2011, 993). This situation is captured by Fuchs political-economy approach to privacy stating “What we have are two sides at odds, a capitalist market which will not be pro-active based on economic justifications operating under a pro-capitalist government with the only power to regulate (set corporations into a reactive mode)” (2011, 304). Moreover, as should now be clear, even these explanations have failed to touch upon the technical aspect of digital privacy or the what happens to commodified information. The technical knowledge required to supplement these arguments, although fundamental, simply does not exist in a capacity other researchers could utilize. The economic orientation then of privacy as a
commodity fails to recognize the significance of the technical infrastructure on which information-based markets rely.

In summary, under this conceptualization, existing research demonstrates a confusion over how to connect the many dimensions contained within digital privacy's relational network. It becomes unclear what elements should be considered fundamental to its discussion or relate back to other forms of privacy. The very conceptualization which is based in digital privacy-discourses still fails to provide a satisfactory way to define it. By seeking to root itself in economic components it generates yet another imbalance of interests in the journey to conceptualize privacy.

7.3.5 Contextually Bound Privacy

The final two conceptualizations of privacy are both considered to be strongly oriented towards the social. They are forms of viewing privacy as signified by the relations between subject level and topic. Contextually bound privacy is viewed as a conceptual form of privacy which recognizes the inherent complexities represented by the sum of previous conceptions. Its primary focus is to establish that desires for control are moderated by a plethora of factors and, as such, seeks to restore a measure of ambiguity to its conceptualization. Under this conception, scholars hold that the context of any given situation, including individual factors and cultural beliefs as an integrated level of subject analysis, hold such strong influences over the perception and definition of privacy that it becomes impossible to develop one universal conceptualization (Smith et al. 2011, 1002). This is based on the acknowledgement that individuals perceive and understand the world around them in a completely subjective manner. So much so, in fact, that the acknowledgement of a violation of privacy is also subject to context. As a result, the way privacy can be defined is limited to actual conditions under which a perception of privacy has been consciously violated as a consequence of a situation playing out differently than what was expected.

Alessandro Acquisti (2004) holds that privacy is therefore a multilayered and multifaceted class of interests which requires any analysis, in order to be accurate, to first identify context before attempting to extract an individual's value calculation. By placing context prior to the individual, a multifaceted approach to privacy includes the addition of numerous simultaneous subject level considerations. Under a contextual understanding of privacy the role of sociability is central to molding how any individual defines a given
situation. Therefore, the analysis of all subject levels (refer to Figure 6.8 in Section 6.6) are to be considered vital for understanding individual perceptions of privacy. Such subjects levels include employment, social groups, family and national culture in addition to any other factors that exist within the immediate environment external to the individual at the time.

According to Bansal et al. context can be related to the type or domain of the research construct: who, where, when, why and with whom becoming discipline, time, location, occupation, culture and rationale (2008). In reviewing the literature using contextual analysis, Smith et al. found that the most often cited contexts considered by researchers were (1) the type of information collected (behavioral, financial, medial, biometric, consumer, geographical, etc.); (2) the use of such information relative to the sector (healthcare, marketing, banking, employer, etc.); (3) political context (institutional factors including a perception towards the right to privacy); and (4) technological applications in regards to future and current capacities (2011, 1003). What this demonstrates, however, is that many researchers using this conception mistakenly choose to exclude more abstract measures of social influences such as peers, family, work groups and broader social orientations.

Helen Nissenbaum is an example of a prominent privacy scholar who is widely accredited with developing the contextual approach to privacy. In her work she attempts to clarify that contextual understandings often mean seeking the ways an individual extends real-world experiences and metaphors to digital environments. Her approach relies heavily on establishing what social and cultural norms mold an expectation of digital privacy norms. In this way she seeks to relate real-world exceptions of general privacy to digital contexts. For example, the expectation of secrecy at a confessional in a Catholic Church would also therefore extend towards any digital confessional space (2011, 38). In the event that no straightforward social precedent exists, Nissenbaum advises scholars to “[start] with ends, purposes, and values and working back from there” (ibid., 44). Overall, it is argued that a contextual approach to privacy would not accept the claim that there is any 'virgin territory' online. Every experience of privacy can be related, in some capacity under the contextual approach, to existing understandings of the world.

In a broad sense, the contextual approach to privacy is one of the only approaches to place a high degree of value on social factors such as norms and general socialization. On one hand, it is a successful conception in the regard that it does account for the plethora of privacy topics across fields and subject level. On the other hand, however, it falls victim to an
over-emphasis of these elements, rendering the overall practice of privacy research incapable of making substantitive claims. By placing individual subjectivity as the most fundamental component of privacy, contextual-based conceptions of privacy become extremely prone to under-valuing other relational elements. This becomes particularly true in its failure to recognize the economic structure of the Internet as dependent upon some degree of produsage. Furthermore, context, as it has been applied thus far, does not lend itself to an analysis outside of individual perception insofar as to describe how a contextual analysis can be used to understand the technical processes surrounding digital privacy such as data-aggregation and analysis. Its subject matter is limited to the actual event of perceived privacy harms and, consequently, ignores the unique elements within digital architectures which cannot be redesigned to meet socially-based desires.

7.3.6 Privacy as Boundaries
In general, the conception of privacy as boundaries refers to the dialectical processes of determining the boundaries of relationships in accordance to the disclosure and use of private information. This relies upon the supposition that the act of self-disclosure, by providing personal information, can only maintain meaning because this infers that some information is deliberately withheld during interactions. What information is withheld and why then functions to define a level of intimacy and, by association, privacy. Therefore, under this conception, in order to study any form of privacy the critical subject matter becomes the contexts of the relationship between an individual and any other entity(s) involved by studying how boundaries are understood by the parties involved. Boundaries, in this sense, infer a type of control over information established by individual rationality and expectations. This notion thus takes advantage of the contextual approach to privacy by allowing for an increased measure of subjectivity in individual perception while providing greater utility by establishing privacy as boundary dialectic with another entity which can be considered to be in relation with the primary subject.

The most fundamental form of this conception is Sandra Petronio's Communication Privacy Management (CPM) theory. This theory encompasses a vast degree of elements contained in privacy while allowing for flexibility amongst discussions. Boundaries, as described by Petrino, define a sense of ownership and control over personal information but can be influenced by personal and collective factors over time (2002). These processes are
viewed as dialectical relationships, experienced in social life as the tension between
experiences of opposites or contradictions. In this way she clarifies the complexity of the
dialectical nature of CPM stating “the basic thesis of the theory is grounded in the unity of
dialectics including disclosure-privacy, concealing-revealing, public-private, openness-
closedness, and autonomy-connectedness” (ibid., 12).

The formation and management of the rules governing disclosure, which define an
individual’s notion of privacy, are broken down into a series of processes. Initially the
construction of these rules are attributed to cultural criteria (including an adapted form of
economic risk-benefit calculation), contextual criteria (life events and circumstances) and
social acquisition. By acknowledging the dynamic nature of privacy, CPM then allows for
these rules to grow and change as individual experiences alter accepted notions of privacy,
forcing their related criterium to be reevaluated. By the measures of CPM, boundaries can
thus factor in the many progressive elements of social life.

Privacy violations, as explained by CPM, are elaborated with a level of contextual
clarity that is not reflected in other conception of privacy. Because boundaries are established
within the complexity of social interaction, it is possible for various types and layers of
boundaries to co-exist within the relational dynamics of privacy. Acceptable levels of
information disclosure then do not have to remain constant across each relationship. For
instance, disclosure can become asymmetrical based on one's desires to share openly without
reciprocation, assumptions based on roles (information given in expected confidence or
secrecy) or accident (unknown boundary overlap such as viewership permissions on social
media). When a mishandling of boundary linkages, ownership or permeability, occur the
tensions this creates requires one or more of the involved parties to reassess their
informational relationship in order to discover what constituted the violations and why. In this
way, privacy violations can be understood as the inability of parties, within a relational
dynamic, to coordinate their privacy rules and boundary management (ibid., 203). In all,
CPM places information into a functional system where once privacy violations have
occurred due to failed information management they can, in return, help renew the system by
increasing an explicit awareness of privacy rules.

In a different, but related, conception of privacy boundaries Eviatar Zerubavel (1982)
locates personal information as central element of social life by defining social distance.
Identifying the various dimensions of personal information to be amount, scope (many pieces
of information of lower quality) and depth (high quality information in a specific area). He specifies that under any given relationship a large amount of information does not necessarily constitute a level of discomfort or violation. It is through the combination of scope and depth that an individual will prescribe a level of intimacy to a specific relational dynamic.

These measures lend themselves well to the digital contexts of online advertising and information gathering which had previously been difficult to operationalize for study. For instance, receiving highly personalized advertisements about a particular subject you are very interested in would be less likely to feel like a violation of personal privacy. This also can explain why a wide-degree of blanketed advertisements based on the contents of a website (i.e. engine ads on a page about cars) are not perceived as invasive because they pertain more to a scope of more general, less protected information. Additionally, Zerubavel identifies pseudo-intimacy to explain that strangers may disclose normally guarded, highly personal, information because they are confident those people will remain strangers and not be seen again (ibid., 102). Applied to the internet, this can evaluate the issues surrounding perceived violations of privacy precisely because an individual expected disclosed information to never be related back to them. However, information gathering tools are non-discriminatory. Thus they gather any and all information for processing without recognition for levels of intimacy unless defined by the servicer ahead of time.

The inclusion of a conception privacy which can be defined by boundaries, established by each party and then dialectically negotiated, provides a powerful tool for the analysis of complexity in privacy dynamics. Situating privacy in a dialectical relationship allows for the presentation and analysis of digital privacy, on any subject level and from any field, given that a relationship can be described. This also resolves many aspects of privacy which can prove to be troubling to understand. As such, privacy violations become an instance for scholars to evaluate the relationship between parties and establish where boundaries were confused/violated either intentionally or unintentionally. This controlled level of subjectivity and higher level of interactional abstraction permits discussions on a boundary based conception of privacy to address any involved element at varying degrees of emphasis. In this way, a boundary based discussion can accommodate other principles of privacy by adding them as elements which help to define perceived and actual privacy boundaries.
7.4 Contested Signifiers of Privacy

The final section of this chapter contains lower level elements of privacy-discourses, identified in Chapter 6, which are currently contested within academic discussion. The question which has arisen is a matter over their purity as signifiers for privacy. Although some are frequently discussed as direct measures for the status of different types of privacy, the logics behind these elements can be questioned. For those researchers who doubt their purity, it is because they see each as something related to privacy but either not a direct source of it or capable of being explained by other, more fundamental, elements of privacy.

7.4.1 Architecture

Briefly, I should like to elaborate on the element of architecture which was discussed earlier in section 7.3.4.5 “Beneath the Veil of E-Commerce”. Architecture, as the coding and systems which compose the infrastructure of the internet, poses one of the most isolated aspects in privacy-related discourse and is nearly exclusive to the domains of information technology and other computer science-related fields. This can be attributed to the substantial differences between the knowledge bases of the technical domain and those of the human sciences, but this disjuncture has potentially significant implications for research.

Many researchers in the human sciences negate the technical possibilities and limitations inherent to the Internet. For example, certain researchers only focus on cookies, web beacons and web logs as the primary means for tracking users. However, this is far from the truth. On-going studies are showing that a great degree of the components downloaded when viewing a web-page are in fact embedded with tracking scripts (Purra 2014) but it has taken exploratory technical research to discover these facts. Furthermore, studies often neglect even the most fundamental issues surrounding cross-site communication, outside of mere “third-party” interactions listed in privacy policies, through the adoption of external elements (social media buttons/icons). The recognition of such elements are essential when discussing facets of control, context and potential privacy solutions. Finding a balance between the technical and human sciences, and thus establishing a dialogue, is viewed as a critical component for future research.

Although technical knowledge and cross-disciplinary writing should be a sought after goal for privacy-discourses, there is a question of how deep into technical infrastructures academics should pursue the study of privacy. There are inherent features of the Internet
which affect privacy, such as web-logs and cookies. But, at the same time, should technical architecture be regarded as central to privacy? This matter can be more complicated than it first appears. While it is true there are inherent factors which impact how privacy, particularly digital privacy, operates within specific contexts, suggesting that privacy is inherent to coding may be an overstatement. Without a literal understanding of what defines privacy, how could programmers successfully operationalize it within the formal composition of coding? This question becomes a matter of defining causality. At the current moment, research cannot definitively state if coding or a lack of transparency in operations creates privacy concerns.

7.4.2 Anonymity

The virtues of anonymity are considered here-forth and placed into question as an actual element of privacy (i.e. is it actually an abstraction of privacy) or if it should be considered a related notion in privacy literature but not a measure of privacy. Anonymity is commonly referenced in privacy literature as an element which enhances a user's privacy by the means of obfuscation, ideally to the point where the ability to be identified becomes impossible. This measure of privacy can be evaluated on a scale regarding how difficult identification becomes. In the political-economy of the internet, anonymity can be seen as a utopian tool of free-speech and a protector of open electoral processes (Solove 2007). Under conditions of anonymity one becomes free of potential repercussion by removing user concerns related to identification online and, in theory, gain the highest potential for open expression. This idea is also attached to the notion of privacy as right, particularly in the United States, by seeking the extension of rights to free speech, the right to be free from unwarranted harassment and/or the right to choose when someone wants to present themselves (Gibbs et al. 2005; Strandburg and Raicu 2006). Anonymity also can be regarded as a sub-dimension in the conception of privacy as a state. Westin (1967) had placed anonymity as one of his four states of privacy along with isolation, intimacy and the information reserve. In this regard, anonymity becomes a desired state, allowing for increased levels of self-disclosure.

Yet anonymity comes with an inherent downside as well. Under the conception of boundaries and relations, anonymity subverts the entire notion by masking the self and expresses a refusal to allow another party to engage in the dialectic of boundary negotiations. A diminished the ability to be identified also reduces a measure of accountability for actions. This can be utilized by anyone with malicious intentions for purposes of committing crime,
spreading harmful or hateful speech and/or other purposes beyond the mere circumvention of oppression or tracking. Literature that is critical of anonymity often subjects it to a cost-benefit comparison, seeking to find a delicate balance between anonymity and accountability (Solove 2007). This balance requires the possible harms and benefits of anonymity to be weighed. Furthermore, within the commodity perspective of privacy, anonymity also subverts the data-based subscription model by permitting a user to mask their data.

When carefully considering these facets of anonymity, it should become apparent how it can be questioned as an element of privacy. Anonymity, itself, fails to fit into the presumptions most models use. This is particularly so for the conceptions of privacy as a commodity and boundary negotiation. Anonymity also does not fundamentally improve or lower standards of privacy. While it may be considered a modifier of control, what anonymity does in reality is subvert privacy. Anonymity is fundamentally achieved through the use of privacy-enhancing technologies (PETs) and the desired use of PETs can generally be considered a reaction towards the failed attempts of national regulatory efforts (Hornung 2013, 184). Although anonymity does have a relationship with privacy, it is not a form of privacy in and off itself. Rather, anonymity can be considered a response to the issues surrounding the current state of privacy without actually addressing the real issues causing privacy concerns. The logical question surrounding this view is if in a perfect state of privacy would there be a need for PETs? Research which begins to touch upon the subject of anonymity should, in effect, be careful to consider anonymity as something that affects privacy online but is questionable as an intrinsic element.

7.4.3 Security

Security has been analyzed both as a social and technical aspect of privacy across literature. These discussions include the use of encryption, protection from cyber-attacks, data-handling practices and the employment of other privacy enhancing technologies as a way to protect personal information. Phrased succinctly by Smith et al. security concerns broadly address three issues: “integrity that assures information is not altered during transit and storage; authentication that addresses the verification of a user’s identity and eligibility to data access; and confidentiality that requires data use is confined to authorized purposes by authorized people” (2011, 996). However, the direct relationship between privacy and security remains unclear.
The threat of hackers and various forms of cyber-attacks can indeed be perceived as privacy threats. When databases are compromised it is often for the purpose of extracting personal information, such as financial details, which can be sold in the criminal underground. Such cyber-attacks are well documented and often make national or global headlines. One report indicates that roughly half of United State's adult population have had personal information released as a result of corporate server hacking (Pagliery 2014). Meanwhile, on the individual level, users are subject to potential threats of malware, viruses and social engineering attacks (Brenner 2010). But the question remains: to what extent should security be regarded as an element of privacy?

Under the conception of privacy as a right there has certainly been a significant degree of legislation passed regarding security on individual, economic, national and trans-national levels. In the United States laws have been established under the Identity Theft Protection Act of 2001, National Homeland Security Agency Act, Computer Security Enhancement Act of 2002, etc. meanwhile the European Union has also created legal frameworks around information security requirements under the Data Protection Directive, establishing uniform cybercrime penalties and cooperative preventative efforts (Bahdur et al. 2002). The legal requirement and enforcement of security standards for data represents an enforced degree of control and establishes ways to define unacceptable data-collection techniques.

Thus security crosses numerous subject levels. This includes topics such as individual personal security and protection (i.e. firewalls, passwords, and updated software etc.), businesses as the protection of collected consumer information and towards the national/inter-national levels reflecting desired degrees of protection. In addition, by the contextual and boundary conceptions of privacy, it is possible to see security as a moderating factor when choosing to opt for a specific level of self-disclosure. Fitting within each model, it then becomes reasonable to accept security unquestionably related to matters of digital privacy. However, it is possible to argue that researchers must make a careful distinction to not regard security itself as a form of privacy.

In order for privacy to exist there must be a certain level of security established and that can be addressed from any conceptual model of privacy discussed. Yet it would not be correct to assume that security is a form of privacy. Security alone cannot guarantee privacy. In fact many information security experts would argue that informational security is never absolute. There are vulnerabilities within any secure system no matter the precautions. The
best that can be accomplished is minimizing the risk of security-related privacy violations (Stewart 2009). Therefore, security is at its best an assessment of privacy risk but not an actual form of privacy itself. This element therefore raises the same concerns stated earlier regarding questions of causality.

### 7.4.4 Surveillance/Dataveillance

Forms of surveillance and dataveillance are undoubtedly prevalent topics in digital privacy research. Specifically, within the discourse surrounding e-commerce and personal data, are concerns over data-mining and tracking. The distinction between these two forms derives from that surveillance is generally a form of actively monitoring an individual through the use of technology or personnel, thus surveillance can associated with the physical privacy as well, meanwhile dataveillance can be more passive in its collection and analysis of data trails left behind during digital activities (Bennett 2011a; Bennett 2011b; Degli Esposti 2014). Dataveillance, however, is not as new to society as one might think. Roger Clarke defined dataveillance in 1988, well before the rise of personal digital technologies, as the “systematic monitoring of people’s actions or communications through the application of information technology” (500). Yet, beyond actual surveillance scholars and the select few researchers, these terms are generally considered synonymous on a basic level as the employment and use of information technologies to track and monitor user behaviors in either an active or passive manner.

Surveillance is a global issue due to the international borders crossed in existing information flows. Adding the issue of global access to web-services, continual technological developments, which are increasing the efficiency and lowering costs of surveillance, have produced increasing levels of mass surveillance which targets groups of people instead of specific individuals (Bennett 2011b). Compounding concerns over privacy in relation to forms of surveillance, the quantity of data to be stored for an indefinite period of time also allows for retroactive surveillance of old data trails (ibid.). Conceptions of privacy as control and a right are regularly viewed as a central area of concern for surveillance scholars. Surveillance is a question of power, governance, global capitalism and impacts upon individuals (Bennett 2011a). As such, there are consistent arguments made which call for regulation by law or highlight the conundrum of government institutions utilizing surveillance (Fuchs 2011).
In contextual and boundary related conceptions of privacy either form of surveillance represents a third-party who's presence may or may not be known. In the former case, context can provide insights into why users alter their behaviors when the presence of surveillance is known. In the latter case, should a circumstance arrive where the presence of surveillance becomes acknowledged after it has begun, a crisis moment arrives for the individual. Contexts would need to be redefined. Relational boundaries would have been directly and intentionally violated, requiring the renegotiation of the boundary rules and management.

Because of the prevalence and general heightened level of concerns surrounding matters of surveillance it is an exceptionally well noted and adapted aspect of privacy research. However, surveillance is an external factor of privacy, often located outside direct subject-level or included as situational factor. This results in the strongest emphasis for surveillance to be in the contextual understanding of privacy despite its common association with notions of law and control. While this may not at first appear as a significant problem for study it raises an issue regarding the purity of surveillance as a signifier for privacy. The point can be made that surveillance is not in itself a signifier of privacy but a bundle of other elements of privacy in a contextually unique package. Such questions theoretically amount to if surveillance should be considered a topic of study which is defined by more fundamental elements such as information use and tracking. Although not a direct issue questioning the validity or use of surveillance studies, this issue is critical for privacy's theoretical analysis when the sub-theoretical notion seeks the most fundamental elements/topics of privacy-discourses.
PART III: Results, Discussion & Conclusions
Chapter 8- Results of the Structural Content Analysis

The sub-theoretical notion functions a bridge by providing a uniform platform unto which existing privacy-discourses can ultimately be evaluated upon. Working from the structural content analysis, it is now possible to begin an extraction of what the actual STN contained across privacy research is. As the SCA from Chapters 6 and 7 organized the elements of privacy into their relational networks, this provided an overview of what the STN of privacy must be capable of addressing along with the questions it should help provide answers to. Successfully deriving a STN of privacy would then explicate the true fundamental conditions of privacy. In effect, a functional STN should not invalidate any of the established literature but theoretically cement how situations of privacy are being discussed as progressions of the sub-theoretical as well as if the correct signifiers are being emphasized. The ultimate value of the STN then becoming its ability to provide clarity.

8.1 The Dialectic for Producing Privacy's Sub-Theoretical Notion

In Section 6.3, Coding to Uncover Levels of Abstraction, the relational dynamics of privacy were coded into four categories. Of these, it was stated the STN would be located within the types of privacy and topics contained in privacy-discourses, then becoming the organizing factors for the SCA in Chapter 7. With each code from the higher elements of privacy now discussed, in addition to their most prevalent lower elements, it is time to explicitly extract the patterns found. The process of deriving the final results of the SCA is thus broken down into two stages. First is to elaborate on the patterns contained within the higher level conceptualizations of privacy, which have described privacy's conceptual refinements as a whole. The second stage is the breakdown of any such pattern into its literal sub-theoretical components. This process is required to supplement the first stage and discover why general privacy has been sub-divided into distinctive physical and digital categorizations. Therefore, we will find the STN of privacy to be a dialectic amongst its conceptualizations and the topics each addresses.

8.1.1 Finding a Pattern Across Privacy's Conceptualizations

The higher elements of privacy as a sub-theoretical notion were discussed within the structural content analysis as the various conceptions of privacy, both as a general definition
and in relation to digital contexts. A general theme of control became apparent throughout the SCA. Originating with Westin (1967), control was established as a means to limit access to personal information. However, as the conception of privacy as control was applied to different contexts Westin himself, as well as other scholars, began to subsume a notion of control within other conceptualizations. The rationalization for this became seeking more refined and “accurate” signifiers to measure specific instances of privacy. As each progressive conceptualization emerged it favored particular fields and sought to explain phenomena from a particular standpoint. The first issues with orders of abstraction thus began to arise as the notion of control became refined under other, more contextually specific, applications to create signifiers with stronger, more empirical, results.

As other scholars returned to and began deriving new ways to conceptualize privacy as control they attempted to increase its perceived explicative power as a scientific tool for analysis. Altman (1975) added a notion of 'selective control' in order to accommodate a reasoning for why various degrees of informational disclosure were being seen across contexts. Meanwhile, far on in the future, Margulis (2003) ended up merging both Westin's original notion of control as 'limited access' and Altman's form of 'selective control' to reflect an individual's desires to maintain a high level autonomy while limiting any possible vulnerabilities. Therein Margulis' definition provides the highest degree of flexibility to account for the social nature of privacy transactions.

Privacy as a state of mind placed its emphasis on the condition of being private as an individual’s sought after goal. This conception thus viewed privacy violations as a break from a desired state of privacy, constituting as a loss of control. Here, privacy maintains a more subjective interpretation based on individual self-perception. However, as privacy literature developed, privacy as a state of mind fell prey to later conceptualizations due to its own ambiguity. Privacy as a state became a psychological factor/element of privacy, rather than a definition, for other scholars to build from.

In the conception of privacy as a right, control was situated within the literal production/enforcement of law. Thus jurisprudence became a primary logic of privacy and the historical ontology of privacy law, providing the frameworks necessary to distinguish how and when privacy would be protected, the primary signifiers. The right of privacy was traced back to Warren and Brandeis' (1890) definition of privacy as the “right to be left alone”. Privacy, when treated as a right, becomes the embodiment of a legally enforceable
ability to control information or the ability to claim one should have control. As such, the privacy as a right conceptualization is generally found seeking to establish the role of governance as moderator between other factors. Focus shifted away from the individual to the balancing of social and economic interests. While this framework is powerful for evaluating the political-economic facets of privacy, the right to privacy only seeks to explore control as an expression of power rather than as a definition. Instead of providing a theoretical understanding of privacy, this conceptualization only helps to highlight and create new questions surrounding the relationships which pragmatically define privacy.

The commodification of privacy was the only conception to be grounded exclusively within the contemporary conditions of information markets. As a conceptualization, it centered around the effects of technological development, specifically, those of the Internet and e-commerce. The conditions surrounding the development and rise of the privacy as a commodity conceptualization are unique in that it came about inductively from actual existing processes. However, the privacy as a commodity conception becomes extremely complex, serving as one of the origins for the emergence of a digital privacy distinction and as one of the original reasons this study was developed.

When considering privacy as a commodity, the first serious mistakes in the assumptions of researchers were found. The inherent complexity of the systems which gave rise to the commodification of information also produce troubling questions of how to limit studies in scope or depth without inhibiting conclusions. As research began to selectively focus on particular elements and their signifiers, a conscious recognition of what was excluded and how this could affect studies was left out by the majority of authors. Consequently, produced knowledge became value-laden with unrecognized assumptions or limitations (Smith et al. 2011). Such was the case with research not recognizing the privacy paradox or technological infrastructure of the Internet.

The privacy as a commodity conceptualization placed its strongest emphasis on economic factors and the technical infrastructure creating emergent privacy concerns. Earlier conceptions of privacy (control, state and right) were all subsumed by economic conditions established through an emphasis on rational-actor models and evaluating individual autonomy. In this manner, although matters of control were still present, the direct notion of control was lost within the abundance of newly refined signifiers: data collection/use, advertising, contracts, exchange and so forth.
Contextually bound privacy in addition to privacy as a boundary negotiations showed a return to individual subjectivity as a means of moderating the fluidity of privacy situations, showing potential for overcoming privacy's ambiguity. Contextually based privacy accentuates the acknowledgment that a plethora of factors, including various levels of sociability (group, employer, cultural and national) as well as other social conditions, moderate how an individual perceives control. However, the degree of subjectivity this conceptualization provides ends up limiting its ability to generalize. While extremely valuable for comprehensive qualitative work, this structural limitation negates the overall goal to provide a definition of privacy in a comprehensive manner while still leaving researchers capable of producing generalizable results. As such, a contextual conception ironically overstates the social and psychological factors of privacy, impeding any pragmatic progression.

Privacy as boundaries, on the other hand, establishes a functional model for understanding how value is assigned by an individual to their personal information. Privacy concerns and violations can then be seen as a dialectical negotiation of boundaries within the framework of relational perceptions. Accepting specific levels of control over information access becomes a defining element of boundary recognition. For example, perceived privacy harms caused by a web-service to an end-user would be explained as the differences amongst their understandings of each other's informational boundaries. For resolution, at least one of the involved parties will eventually have to come to terms with and reformulate their understanding of permitted levels of access within the existing relationship. Overall, this conception of privacy can be seen as a balanced understanding of privacy in so far as it concerns socially based elements. Its limitations, however, are in that the conceptualization has yet to be developed to a point where it can fully accommodate digital contexts and passive systems of data collection/analysis. Accounting for all possible relations within a digital environment, seen and unseen as well as known and unknown, would create a vastly complex web of relations under the conceptualization of privacy as a boundaries; no less complex than trying to depict digital privacy without it. Furthermore, it is premised, once again, on an understanding of privacy without explicitly defining what privacy is beyond its own signifiers.

All together the structural content analysis revealed the various strengths and weaknesses of how conceptual elements of privacy fit together. The common theme found
was one based in a way to measure degrees of control and the factors which influence it. In addition, it was seen that in order to produce a single conception of privacy it must be capable of providing a means for measuring all levels of subject analysis from the social to the technological in addition to explaining every debate over emphasis and the origins of its signifiers while remaining simple enough to not match privacy's existing complexities. With this knowledge in hand and a pattern recognized it is now possible to apply Brown's sub-theoretical notion to finally attempt deriving an answer for privacy's missing theoretical foundations.

8.1.2 The Higher Elements of Privacy as a Sub-Theoretical Notion

Michael E. Brown describes the sub-theoretical notion as the “the life of the concept” (2014). It becomes something which is lost as theoretical progression seeks to reduce a concepts ambiguities (ibid.). From the structural content analysis it has become apparent that as privacy has gone through its cycles of refinement each conceptualization ends up merely detailing what to evaluate and explain privacy as through specific signifiers. What each failed to do was actually provide a definition of privacy. Therefore, we find that even the most utilized of conceptualizations have failed to actually provide a theoretical understanding of privacy not rooted in its own signifiers. However, in the process of explicating this through the structural content analysis, a pattern has emerged with control present across every conceptualization.

Control stands as the one aspect of privacy-discourses which was never reduced further from its initial conceptualization. Rather, it was from control that a logical progression was shown across privacy's conceptualizations. In this sense, control was developed as a signifier in numerous ways but control itself was never reduced. Therefore, as we revisit the qualities of a sub-theoretical notion described by Brown we can find that control is the first sub-theoretical notion of privacy. Control stood as an irreducible and irrepressible element across every conceptualization. Whenever control was not addressed in a direct manner this was due to its radical transformation into another signifier or the fact it had been taken for granted as an element logically prior to what was used as its representation. Various conceptualizations had taken control and attempted to reduce its ambiguity to design signifiers capable of producing more concrete explanations of specific phenomena. Thus as theoretical progression occurred, moving privacy further away from a foundation based in
control, conceptualizations moved altogether from what privacy is towards what privacy describes. As this occurred, attempts to reduce the ambiguity of control also reduced privacy's applications to the conditions of life therefore resulting in contextual complexities as limitations. Control stands as a fundamental aspect of social life and is thus capable of explaining every element identified within privacy-discourses.

However, “control” itself cannot stand as a perfected sub-theoretical notion for privacy. This is because control without any other conditions merely describes rather than defines. To find out why this is true we can revisit the developments of control as an independent conceptualization of privacy. In Alan Westin's original definition of control he describes privacy as the “claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (1967, 7). Irwin Altman then built from this to define privacy as “the selective control of access to the self or to one's group” (1975, 24). The key shift here, and then later in Stephen Margulis' own definition, is defining privacy specifically as access to information. The question then about control, specifically within privacy, is not just control but who has control.

Once the matter of control has been shifted to a question of who has control it is possible to move forwards to address the complexities contained within privacy research. Further conceptual developments in privacy involved control but needed to refine it in-order to provide concrete explanations for who had control and how. Digital privacy, as the most complex contexts for researchers, is then the specific conditions which must be clearly defined by control to become a satisfactory STN. However, what became apparent under the conceptualization of privacy as a commodity was when addressing digital privacy there are unclear dimensions of who has control and how much. Control over informational access was gained by those using privacy enhancing technologies. Control was lost under the conditions of adhesion contracts used by online services but the role of law could moderate this by establishing a right under specific circumstances to have certain information kept private. Overall, the technological infrastructure of modern economics, and thus information commodification, obscured the conditions of privacy to the point where it becomes reasonable to assume relational dynamics concerning who has control over information and how much are almost impossible to identify in their entirety.

Taking these facts into consideration, there must be a way of phrasing control which
can explain the entirety of existing privacy contexts or else control cannot be a sub-theoretical notion any longer. Relief from this distress comes from taking back into consideration the problem of who has control and how much. With other elements and relations of privacy altering these factors, the conditions of privacy are not about control itself but to whom control over access to information is given and how much. Therefore, the sub-theoretical notion of control can be completed by altering its phrasing. The true sub-theoretical notion of privacy becomes the loci of control. Now, as a STN, the loci of control is capable of expressing conditions of ambiguity over who has control over access to information by adding a degree of flexibility capable of describing various amounts of control over information as reflected in the totality of privacy situations.

8.1.3 The Lower Elements of Privacy as a Sub-Theoretical Notion

While it is tempting to leave privacy's sub-theoretical notion at the loci of control this would only answer what composes the theoretical foundation of general privacy. The foremost identified issue of conceptualizing privacy was that a rift has formed between physical and digital situations of privacy where the chasm in-between them represents general privacy. Alone, the loci of control does not provide a sufficient explanation as to why privacy researchers erected a distinction between digital and physical forms of privacy. It would not be a satisfactory to simply state digital privacy has more complicated relations regarding who has how much control over information. This answer would leave the fundamental question of why unanswered. As such, it can be realized that alone the loci of control is still incomplete as a sub-theoretical notion for privacy. Therefore, to answer the remaining research questions, it becomes necessary to go back to digital privacy and, its historical predecessor, physical privacy to discover what has altered the loci of control dramatically enough to cause this division.

In the structural content analysis, it was recognized that the privacy as a commodity conceptualization was rooted exclusively in explaining digital privacy and it is therefore the critical point to begin answering this question. Within the privacy as a commodity conceptualization, its unique factors were in its emphases on modern economics and technological developments. Because these domains were essential to developing the fundamental conditions for the commodification of personal information, thus creating digital privacy concerns, it is somewhere within these factors that it becomes possible to find what
changed about the loci of control. Therefore, we must again refer to the lower elements of privacy, which composed the various topics/signifiers surrounding digital privacy, to discover what, in relation to economics and technology, has caused change.

Going back to Figure 6.6 the lower elements of privacy which are exclusive to matters of digital privacy are data-mining, defaults, encryption and web tracking. Predominate elements also brought up in the privacy as a commodity conception add matters of security and surveillance, specifically dataveillance. What do all of these elements have in common? They all regard the collection, use and access to information but these things can all be explained as matters of privacy by the way the loci of control is allocated. The concern here is what is different between physical and digital matters of privacy. So then we can rephrase the question to be: why can these specific elements not be physical?

While of course they are all inherently digital what makes them digital is that we are not discussing the same types of information anymore. When information is digital it becomes data. Therefore the question can be further refined to be about what makes data unique from physical information. Data is unique because it can be composed of any action or information placed online and, more importantly, it is atemporal. Access to information which has become data does not require one to be present at the moment the information is created. Furthermore, such data can be copied, stored and processed by any number of computers simultaneously.

While it is certainly true that these qualities make data more easily accessible, access to information is still covered by the loci of control. The sub-theoretical notion of data then, as a sub-component to privacy's STN and modifier of control, must be something outside of mere accessibility. What fundamentally makes data so easily accessible as compared to physical information in an irreducible and irrepressible manner? The answer to this question is a rather abstract notion itself: tangibility.

When addressing tangibility as a sub-theoretical notion what is being considered are the distinctive differences between physical and digital information/data. Tangibility, in its traditional sense, refers to having physical existence which makes it a difficult term to grasp when the point being made is that data is more tangible than physical forms of information. However, what we are looking for to complete the STN of privacy is not a term exclusive to either physical or digital forms of privacy but both. Tangibility, when describing data, is used as a reference to the properties of data which make it more easily accessible and re-purposed.
than physical forms. This can best be elaborated by its actual applications.

When an individual goes outside and spends the day wandering around from place to place to find out where exactly this person has gone and what they have done is a feat. Without having this person under surveillance or being capable of piecing together eye-witness accounts it would not, in all likelihood, be possible. As time passes between the events in question and the start of an analysis its difficulty grows exponentially. Now add technology to the mix with the conditions of gathering and recording information in the form of data. In the physical world, GPS and other elements of locational privacy make it possible to see exactly when and where this person was. Imagine, instead, this individual stayed indoors but went from place to place online, making posts on social media and shopping. Their digital trail could not be easily erased or covered. Online trackers and web logs would make countless entities privy to everything that occurred with time, location and content. This data could be gathered, sold, exchanged and/or analyzed with nearly no effort, a great portion of it being entirely automated. In this sense, data is more tangible than physical information.

Tangibility as a sub-theoretical notion is a specific reference to the ease of which information can be gathered, copied, distributed, commodified and/or refined. This works in tandem with the loci of control to describe the conditions regarding how easily information can be accessed and used in various ways. It is thus the tangibility of information which can provide an ambiguous but irreducible and irrepressible condition of privacy which modifies the loci of control to the point in which the distinctions between digital and physical privacy can be explained. Measuring tangibility becomes the matter of refining it in coordination with the loci of control to get signifiers that deliver measurable concrete explanations for specific situations of privacy. Combined the loci of control and tangibility of information compose a complete sub-theoretical notion of privacy which can describe any given situation of general, physical or digital privacy by creating a solid theoretical grounding for conceptual development to occur from.
Chapter 9- Discussion

9.1 The Significance of the Findings for the Human Sciences

Arriving at the sub-theoretical notion of privacy allows for the domains contained within the human sciences to critically reflect upon their own assumptions when measuring phenomena related to privacy. One of the core issues related to the complexity of privacy came about from an over emphasis on economic factors when looking at the affects of technological innovation. Digital privacy is being predominately defined by the commodification of privacy. However, now looking at the STN of privacy, the privacy as a commodity conception becomes fundamentally flawed because it locates the origins of digital privacy primarily within systems economics. But systems of commerce, including notions of property and value, themselves are based in other more fundamental but less refined elements of society.

Other conceptualizations of privacy fell victim to the same forms of confusion by using notions which were fundamentally predicated in other aspects of social life to define privacy. Privacy as control and a state were the two conceptualizations closest to the STN of privacy but these conceptions became overly refined in their attempts to accommodate further relational dynamics of privacy. Privacy as right ended up merely explaining privacy as expressions of power in relation to systems of governance but failed to identify what about those systems actually composed privacy. Contextually bound privacy and privacy as boundaries overstated the social components of privacy creating definitions of privacy which were too complex to adequately explain any ubiquitous conditions which created situations of privacy.

Taking the sub-theoretical notion of privacy as a more general lesson about what signifiers used to measure phenomena represent, this study provides reasons for the human sciences to critically gauge their contained assumptions and what effects these assumptions have on any substantiated claims. It may very well be the case that when a subject faces immense challenges bridging numerous studies this is due to an incorrect theoretical foundation and absence of an acknowledged STN. But more than this, employing the sub-theoretical notion to provide new theoretical groundings for conceptions represents a return to the human sciences as a way of unifying the different domains of academia.
9.2 The Significance of the Findings for Media and Communication Studies

For Media and Communication studies (MCS) the sub-theoretical notion of privacy can provide critical insight at how to consider the ways situations of privacy may be involved in research. The relational dynamics, established by the structural content analysis, attached significance to privacy in nearly all corners of communication both as a social action and subject-matter. It can prove valuable for those within MCS to consider how these dimensions of privacy could potentially influence their own research. While this could alter the way a MCS researcher addresses a specific topic, this also lends itself as a manner to foresee any ethical concerns over privacy.

When researching people's communicative habits and actions there is an inherent factor of privacy relevant to the subject-matter. Digital and physical information come with an attached expectation of privacy. When the ability to freely access is generically considered the equivalent of consent countless issues can arise. Typically legal consent to do a study on information contained within a social media site, or any site hosting the information of others, can be given by the host. However, as this study has shown, an understanding of privacy is not always reflected in legalities. By instead considering where the loci of control is located and how tangible the data is in respect to the original owner/creator researchers can garner a greater understanding of how privacy might be perceived in the contexts of a study. By being considerate of this, potential reputational harms can be avoided.

9.3 Reflection on Methodologies

As an exploratory and initial case for the direct employment of a structural content analysis to derive a sub-theoretical notion there are a few issues this study encountered which can be improved in future research. The inherent limitation of these methodologies is that the study itself is an inductive process for discovering an underlying logic. Being an inductive methodology, the results are designed to fit within the studied literature. However, to achieve greater measures of validity requires the future use of this STN of privacy by others across further examples of research.

The sub-theoretical notion, as a new analytical tool for theory, also required the employment of an additionally unique methodology. While the SCA and STN were essentially designed to work in tandem, making them the ideal methodological choices, they are both undeveloped in academic research. This holds particularly true for structural content
analyses which face some inherent problems regarding transparency. On one hand, its
greatest value is in providing a way for researchers to comprehend an incredibly vast amount
of knowledge, regardless of complexity, in a respectively short period of time through active
engagement. On the other hand, this active engagement, via a structural outlining of the
sampled texts, made explicating the process of coding extremely difficult. To provide
sufficient transparency in the process of deriving codes would ideally mean showing how all
the coded elements came together. However, even this study the refined sample was over a
hundred pages of text. Showing basic examples for each final code representing a relational
dynamic would have composed the majority of this text. Overall, considering the complexity
and ambiguities involved in the study of privacy, as well as the incredible scope of involved
research, this choice in methodologies served the purposes of this project extremely well. It is
possible that with a less complex topic both the SCA and the derived STN would be easier to
explain with an increased level of transparency.
Chapter 10- Conclusions and Implications for Future Research

10.1 Privacy as a Sub-Theoretical Notion: The New 'As Things Stand'
Seeing the loci of control and tangibility of information as the completed sub-theoretical notion of privacy we have finally arrived at a theoretically grounded platform on which the totality of privacy-discourses can be reevaluated and built upon. By first seeking to understand privacy in its entirety through the dynamics of its contained relationships under the structural content analysis and then deriving what the emergent patterns meant, it is now possible to clearly explicate the current standing of privacy. This is a direct result of identifying the sub-theoretical notion of privacy and what, over academic development, caused the study of privacy to become so complex.

General privacy became lost in privacy-related literature as the historical and cultural conditions of societies shifted due to technological development. Although general privacy should stand to define privacy as a whole and encapsulate all other forms, it instead became a disconnected and floating meta-concept of privacy research. While historically there had only been matters of “privacy” as its relational dynamics developed, and researchers sought further refined conceptual developments to produce more concrete explanations, this inadvertently began a trend of distinguishing particular sub-classes and forms of privacy as unique. With the advent of digital computing and its proliferation across all matters of social life, the broad distinctions of digital versus general privacy erupted as a fissure within general privacy research. However, these distinctions were not as blatant once turned inwards towards the identification of their fundamental differences outside of contextual subject-matter and within their irreducible basic conditions every one of their signifiers represented.

It is here that the exact location and amount of control became a nearly glaring uniform condition for all discussions of privacy. Yet, the loci of control only was capable of tying together the conceptualizations of privacy, not explicating why divisions had erupted. To answer this, a secondary sub-theoretical notion was required which could explain what worked in tandem with and modified control. Isolating what of the subject-matter contained under digital privacy, studied predominately under the privacy as a commodity conceptualization, this was precisely located in the fundamentally changed qualities of information as an effect of technological development. Thus we can find the answer as to why digital and physical privacy became disjointed as explained by changes in the tangibility
of information. Where digital information, as data, expresses unique qualities unlike physical information, which enable its rapid, simple and aggregate collection/use outside of time or presence of whom it pertains to.

It is now possible through this sub-theoretical notion of privacy to address where privacy research has developed from and evaluate where it stands today. Existing conceptualizations of privacy, discussed in Section 7.3 and evaluated in Section 8.1, are not singular definitions of privacy but refinements of the sub-theoretical. Rather, these conceptions are theoretical approaches which evaluate particular relational aspects of privacy, designed for specific investigatory goals. They provide frameworks, each with their own groups of assumptions and specific emphases, that highlight which refined signifiers are to act as central measures of control and tangibility. The key distinction then, regarding privacy-discourses, is that existing research has been predicated on the confusion of mistakenly utilizing ungrounded conceptualizations of privacy as definitions. Therefore, emerging theories could only seek to explain specific situations or forms of privacy because they lacked a fundamental understanding of privacy which could act as a universal definition.

10.2 Implications for Future Research
Should future research begin to accept the theoretical foundations of privacy as the loci of control and information tangibility then the totality of this area of research can begin to move forward from its struggles over privacy's inherent ambiguity and resulting complexity. Theorists can begin to use the sub-theoretical notion of privacy to design new conceptualizations which now have theoretical grounding and substance to build from. Researchers can then utilize this grounding to circumvent the complexities and debates of existing research to relax in the comforts of being able to openly produce valid research within their own theoretical explanations of privacy situations. Rather than stumbling over attempts to explicate the superiority of one approach to privacy, the sub-theoretical notion can provide the means for recognizing common grounds. This makes all privacy research inherently interrelated under their refinements to measure the loci of control and tangibility of information; therefore resolving existing issues of inter-disciplinarity and cross-disciplinarity in research.
10.3 A New Personal Agenda for Privacy Research

The arrival at the sub-theoretical notion of privacy has provided me with a new goal as a researcher. With the initial intentions of this study to be the generation of new conceptual models for privacy rather than just a theoretical foundation of privacy, these concepts are currently in development. An on-going process arrived at from this study is the introduction of data-based privacy and information-based privacy as new conceptual models to replace the mangled and confusing uses of digital and physical privacy in future discourses.
References


the Surface of Data Mining.” *Journal of Business Ethics* 40(4): 373-86.

78(4): 1607-60.

Ithaca: Cornell University Press.

Degli Esposti, Sara. 2014. “When big data meets dataveillance: The hidden side of analytics.”


habits.html.

“Examining Internet Privacy Policies Within the Context of User Privacy Values.”

hidden-perils-of-cookie-syncing/.

http://newsroom.fb.com/company-info/.

Fox, Margalit. 2013. “Alan F. Westin, Who Transformed Privacy Debate Before the Web Era,
http://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-
privacy-dies-at-83.html?pagewanted=all&_r=0.

Fuchs, Christian. 2010. “Labor in Informational Capitalism and on the Internet.” *The
Information Society* 26: 179-96.


Massachusetts Institute of Technology. 2014. "Who's using your data? New technology to track how your private data is used online." ScienceDaily, June 13. Accessed June 18,


http://dataprivacylab.org/projects/identifiability/.


Vila, Tony, Rachel Greenstadt and David Molnar. 2003. “Why we can't be bothered to read privacy policies models of privacy economics as a lemons market.” published in Fifth International Conference on Electronic Commerce (ICEC): 403-07.


118
APPENDIX A
Selected Texts Listed in Bibliographic Order


**APPENDIX B**

Selected Text Categorization By Dominant Discipline and Genre

(Listed in Order from Appendix A)

<table>
<thead>
<tr>
<th>Book</th>
<th>Categorizations</th>
<th>Genre</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Discipline(s)</td>
<td>General</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Book</td>
<td>Categorizations</td>
<td>Genre</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Discipline(s)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>General</td>
<td>Social Sciences</td>
</tr>
<tr>
<td>16</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>