LEAVE ME ALONE: PROTECTING CHILDREN'S PRIVACY IN THE DIGITAL AGE

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirement for the
degree of
Master of Arts
in Communication, Culture and Technology

By

Katherine A. Hild, M.P.P.

Washington DC
April 11, 2017

LEAVE ME ALONE: PROTECTING CHILDREN'S PRIVACY IN THE DIGITAL AGE

Katherine A. Hild, M.P.P.

Thesis Advisor: Evan Barba, Ph.D.

ABSTRACT

Although considerable research exists on the social norms and habits of teenagers in online spaces, information about parental knowledge regarding data privacy protection is limited. While the privacy challenges of social media platforms or commercial advertisers are clear to many parents, the growing popularity of non-traditional connected devices, often referred to as the "Internet of Things," presents additional challenges in the form of toys and household objects that now collect data from their children. Through a series of semi-structured interviews with parents of children ages 5-17, this thesis examines how parents understand data privacy, as well as how their understanding subsequently influences the behavior expectations and device usage policies they set for their children. Topics discussed with parents include their familiarity with: state and federal privacy legislation aimed at minors, such as COPPA or FERPA; data-tracking technology like cookies; data privacy protection functions available on mobile devices; privacy tools such as ad-blocking extensions; and high-order privacy threats like hacking or doxxing.

A heartfelt thanks to Dr. Evan Barba for all his help in this process,
to Leslie Harris for her additional assistance,
and to Dr. Jeanine Turner for always offering an extra shoulder to lean on.

To my friends and family:
thank you for your constant support and encouragment on this journey.
I couldn't have done it without you!

Katherine A. Hild

TABLE OF CONTENTS

I. INTRODUCTION

One day, in the spring of 2011, I received a Facebook notification that I had been tagged in a post made by one of my current students at the boarding school where I was a resident advisor. Curious, I clicked through to view the post, only to be horrified by what I saw: my name had been generated in a prompt by a popular Facebook app called "The Truth Game," in which app users receive randomly generated yes-or-no questions about the people in their social networks. The student had been asked, and was now discussing with multiple classmates, all of whom were under 18, to speculate on a vulgar statement about my sex life.

My immediate response was to try to block the application's access rights; as someone in a position of authority over minors, I did not want my name attached to theirs in such a dubious context, especially on their public pages where I had no control over how they chose to generate or share the content. Yet, Facebook's blocking capability only extended so far: I could stop the game from displaying posts in my own newsfeed, but I couldn't actually prevent it from using my name or profile photo as a "gamepiece" for other users to play with. Indeed, the game's access rights explicitly stated that it had permission to read all publicly available content by anyone in the friend network of the person who played it. My only option to protect myself against this undesired use of my identity, it seemed, was to unfriend anyone who played the game.

As the above example demonstrates, lack of control over the use of our personal data by corporations and third parties is a significant problem in the early 21st century. This concern has increased during the course of my research journey, as the 115th Congress of the United States voted in March 2017 to strip the Federal Communications

Commission (FCC) of its ability to restrict how Internet Service Providers (ISPs) can use or resell customer data (Fung 2017). While the data gathered by ISPs is not necessarily "personally identifiable" in the historic sense, like an address or Social Security number, in 2016 the Federal Trade Commission (FTC) had recommended broadening the definition of Personally Identifiable Information (PII) to include any data that can track individuals across platforms and over time, such as users' device IDs, static IP addresses, online cookies, and location data, "when it can be *reasonably linked* to a particular person, computer, or device" (Rich 2016, McMeley & Seiver 2016). To address this, the proposed 2016 FCC protections had also included new rules that required providers to "strengthen safeguards for customer data against hackers and thieves," which have been voided as well (Fung 2017). Given the rising popularity of non-traditional wired devices like watches, thermostats, and even children's toys that also gather intimate data about our lives, the federal decision to decrease transparency regarding how individual data may be used, sold, or aggregated by complete strangers is concerning.

And yet, this battle between commercial enterprise and individual privacy protection is hardly new; indeed, we have been fighting it since the birth of modern consumer culture in the 1930s (Montgomery 2007, pg. 13). Inherent in the early development of this consumer culture was the notion of targeted advertising—and, more specifically, the establishment of children as a distinct class of consumers toward which to focus advertising. The extension and breakdown of childhood into multiple phases was itself the product of marketing: "teenagers" were not a distinct class of children until the 1940s; "tweens" were invented in the 1990s (Montgomery 2007, pgs. 14-21). Upon recognizing that children were a powerful market force, advertisers began to strategically

brand them as distinct segments of the population, recognizing that they could build enduring product loyalty to these "consumers-in-training" by capitalizing upon their developmental immaturity (Montgomery 2007, pg. 15).

With the rise of the Internet in the 1990s, and the multiplication of wired devices in our lives over the two decades since, we have created an environment in which we unconsciously generate vast amounts of data about ourselves: no longer just our names, addresses, and contact information, but also data concerning our health, well-being, and innermost thoughts. And while some of this is information we share voluntarily, when we interact online we also leave behind digital footprints that we may not even realize, let alone be able to control. Given that privacy plays a large role in shaping our sense of self, the inability to retain control over our data or even to know who is accessing it, has a profound impact on identity, both for individuals and for society as a whole (Kupfer 1987).

The United States has historically placed a high value on individual privacy, particularly against government intrusion, and Supreme Court cases like *US v. Jones* (2012) have established that some types of data aggregation by law enforcement violate our reasonable expectation of privacy. In her concurring opinion, Justice Sotomayor noted that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations" that can provide data about an individual indefinitely (*US v. Jones* 2012). In a similar vein, the First Circuit Court ruled in 2016 to expand the application of the Video Privacy Protection Act to cover consumers of digital media, specifically focusing on GPS data as "personally identifiable," (*Yershov v. Gannett*

Satellite Information Network, Inc. 2016). Despite the judiciary's acknowledgment that there are potential privacy risks associated with digital data collection by both government and commercial entities, the United States lacks unified legislation to protect individual privacy with regard to commercial data collection and aggregation. Legal scholar Daniel Solove warns that our national privacy laws "remain in grave need of an update," noting that there has been very little new legislation since 2000 other than amendments to existing laws (Solove 2017). Our national approach to privacy law has been piecemeal, focusing on specific domains like health, finance or education, rather than on whole people, the way that privacy laws in other Western countries do.

Minors—that is, youths under 18—are the only age demographic that is protected under specific data privacy laws, but even these are limited in scope. All minors are covered under the Federal Education Rights and Privacy Act (FERPA), which protects the privacy of student educational records and gives parents some control over how that data is used (FERPA 2015), and under the Children's Internet Protection Act (CIPA), which requires federally-funded schools to protect students from harmful online content (2000). Additionally, children under 13 are protected against intrusive data collection by commercial websites under the Children's Online Privacy Protection Act (COPPA), which requires parents to give "verifiable" consent in the form of a signature, verbal confirmation, or credit card purchase in order to acknowledge that the site or service will collect the child's data, but this legislation does not extend to teenagers (FTC 2013). Nine states have passed additional legislation specifically focused on aspects of data privacy, but only Delaware and California have passed legislation that addresses data collection and advertising to minors, with California's law not only including teenagers, but also

extending them additional rights to have their content erased from any given site or platform (CA Legis. 2013).

SB-568, known as "Privacy Rights for California Minors in the Digital World," expands upon federal legislation by placing restrictions on targeted ad content served to users under 18, and also requires sites or apps aimed at minors to remove a young user's data upon request (CA Legis. 2013). In its coverage of the bill, Southern California Public Radio cited a 2010 Wall Street Journal investigation finding that uncovered "30 percent more cookies and other tracking devices on the top 50 websites for children and teens when compared with general audience sites," indicating that behavioral data from children and teens was being specifically targeted (Aguilar 2013). Legislators involved with SB-568 cited the developmental immaturity of minors as a primary motivation for creating the bill. Psychological research has shown that children and teens are not cognitively mature enough to gauge long-term risk or grant informed consent in the same ways as adults, and that children and teens are also less capable of curbing impulsive behavior, which can lead to them making poor choices even when they are intellectually aware that they're making a mistake (Casey, Getz & Galvan, 2008). Given the permanence of online content, former California Senator Darrell Steinberg explained that the legislation was necessary to protect the futures of teens, who "deserve the right to remove [ill-advised material] that could haunt them for years to come" (Aguilar 2013).

Given these vulnerabilities, there has been considerable research over the past decade on what minors, and especially teenagers, are doing online when they use the Internet or specific media platforms. The parental components to most of this research, however, tend to focus on whether or not parents feel confident in their ability to keep

track of their children's online behavior, rather than on data privacy or protection. Survey data from Pew Research Center (Pew) and the Family Online Safety Institute (FOSI) collected between 2012 and 2016 indicates that both minors and their parents are primarily concerned with inappropriate sharing behavior that affects the child's standing in their immediate community or social network, which is a marked shift from third-party data collection as the main parental concern expressed during 1990s and early 2000s (Anderson 2015; FOSI 2014; Madden, Lenhart & Cortes 2013; Montgomery 2007). While parents in the 2010s still recognize commercial tracking as a threat, FOSI's survey and focus group research reveals conflicting levels of parental concern: a 2014 report found that parents did not consider data collection a "potentially harmful" choice during one portion of the study, but 57% of parents later reported negative attitudes toward the idea of companies tracking their children for advertising purposes. When asked to rank their biggest concerns later in the survey, "commercial tracking" ranked second, despite the fact that both FOSI and Pew's research concludes that parents are primarily focused on safety, not privacy, when it comes to how they monitor or supervise their children online (Anderson 2015; FOSI 2014; FOSI 2015).

One of the more striking findings of FOSI's "Parenting in the Digital Age" study is that parents rely on teachers as a primary source of information about how to protect their children online, and that they trust schools to help educate their children about technology use more than any other source (2014). A pilot study I conducted in 2016 confirms this finding. In the study, I interviewed New Jersey teachers and administrators about student media literacy and whether or not existing state standards were sufficient to prepare students to be informed participants in digital spaces (Hild 2016). One comment

that came up consistently throughout the interviews, particularly among professionals who worked with pre-teens, was that parental ignorance frequently contributed to privacy, safety, and behavioral problems on the part of their children (Hild 2016). Literature focused on media literacy education also cited lack of research into parent knowledge when suggesting areas for further study (Christopher 2014; Hayes 2014). The results of this pilot study, coupled with my own decade of experience working with children and teens, motivated me to conduct additional research on how parents understand new media issues, with a specific emphasis on data privacy.

This thesis makes the argument that parents lack sufficient understanding of how their children's data is collected or used by third parties through examination of the following research questions: *What do parents know about data privacy issues or policies that are relevant to minors? Where do they typically learn this information? And, finally, how do they communicate this knowledge when they engage with or instruct their children on the use of online devices or social media platforms?*

The goal of this project is twofold: 1) to establish a baseline of parents' knowledge regarding data privacy, including not only their awareness of state and federal privacy policies that impact their children, but also their knowledge of privacy threats and tools they use to control the data footprints that their children leave online; and 2) to understand how parents learn about and communicate their concerns to their children so that more effective tools may be developed to increase parental awareness regarding the handling of their children's data.

Following this introduction, Chapter 2 will establish a framework for understanding privacy in the United States, with specific attention to privacy legislation

that affects children and teenagers. Chapter 3 examines the literature related to how parents and their children understand privacy and safety in online environments. Chapter 4 discusses the justification for this study and the methods used to gauge parent understanding of digital privacy issues that affect their children. Chapters 5 and 6 present the data gathered from my interviews with parents and examines the implications. Finally, Chapter 7 offers concluding thoughts on the ways in which parents understand online privacy concerns that pertain to their children, as well as suggestions for areas of further research.

II. WHAT IS PRIVACY, AND WHY DO WE CARE?

2.1 Understanding Privacy in the United States

Despite being considered something of a universal human right, a clear definition of "privacy" remains elusive in many respects. The United States was conceived on the principles of individual liberty and freedom from state intrusion, and valued so highly that certain privacy rights have been woven into our cultural identity since the nation's earliest days. And yet, despite codifying privacy protections against things like unwarranted searches or self-incrimination, the need for an all-encompassing "right to privacy" was not established until a century later, as intrusive journalistic practices and technologies like the camera and telephone became commonplace, and began to affect people's lives in new ways (Whitman 2004, Solove 2007). Given these shifts in how individuals understood their rights to life and liberty, Samuel Warren and Louis Brandeis articulated that privacy in the modern American sense had now expanded to become the right "to be let alone" (1890).

But from whom or what do we wish to be left alone — and why? In *Configuring the Networked Self*, Julie Cohen suggests that our idea of what constitutes private space or private behavior varies depending upon the environment in which we live (2012). Since we as individuals are part of social networks, we understand privacy through the interchange between ourselves and our cultural environments, in which we "perform" our identities according to social scripts and conventions. We develop a sense of privacy when we make decisions about which personal information we disclose in social situations. For example, there are social situations in which we expect others to understand that our actions or words are private, such as when we speak to a doctor or use

a shared restroom. At other times, such as when we enter public spaces like restaurants or shopping malls, we understand that our words and behavior may be observed or recorded by others. Related to these cultural norms, Cohen (2012) also argues that we define ourselves, and our senses of privacy, in accordance with our cultural *interactions*: our production and consumption of art, media, and intellectual ideas also shape how we understand social exchanges and the boundaries between ourselves and others (ch. 6, p. 2-4). This notion is further enhanced by applying Helen Nissenbaum's (2004) lens of "contextual integrity," which "ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it" (p. 101).

Given that privacy of the individual cannot be understood without a group and a set of cultural values to which individuals can compare themselves, I offer this contextual definition of privacy: it is the idea that certain activities, thoughts or beliefs are, or should be, protected from oversight or intrusion by others.

Privacy plays a significant role in shaping a person's sense of self, and as such is frequently associated with individuals, but it is also possible for groups to engage in private acts, or at least in acts where there is a presumption of confidentiality among the participants. Additionally, privacy norms are often constructed from agreed-upon sets of beliefs and values, not all of which are immediately comprehensible to an outside observer. One does not necessarily know what the boundaries of "private" are until they are intruded upon. Nowhere are we more attuned to this murky boundary than at the digital divide — the area where our long-held cultural beliefs about privacy and social behavior come into contact with new platforms for interaction that are capable of learning

more personal information about us than ever before. Our social interaction in online spaces — which are generally considered public — via personal devices like laptops, tablets, and mobile phones, which are often used within the private space of one's own home, tests our collective ability to renegotiate the boundary of what information about our lives is, in fact, private. The presence of additional Internet-connected devices like watches, fitness trackers, thermostats, televisions, and even children's toys that collect personal data within the privacy of one's home, have muddied the water even further.

2.2 Understanding Privacy vs. Safety

When it comes to data protection in an online context, it can be difficult to distinguish the need for *privacy* from the need for *safety*, especially when young people are concerned. Many parents worry about how their children behave online, and whether their children's voluntary disclosures of information will result in physical or psychological harm. While these are justifiable concerns, worrying about a child revealing their name or address to strangers they might encounter is qualitatively different than worrying about the implications of one's children living under constant third-party surveillance in the form of data-mining and data-trafficking.

The former concern is an issue of safety, here defined as protection against danger, risk, threat, or injury. The latter, however, is an issue of privacy, here understood as the state of being free from oversight or intrusion by others. As stated previously, this extends not just to our activities but also to our thoughts and beliefs.

2.3 Navigating Privacy Rights in Online Spaces

To understand the changing cultural context of our sense of privacy, Daniel Solove explains that "[g]ossip used to travel in local circles. It rarely spread widely and would be forgotten over time. On the Internet, however, gossip … [and] shaming online [create] a permanent record of people's past transgressions — a digital scarlet letter" (Solove 2007). While these long-lived privacy intrusions by non-government actors raise privacy concerns for all people, children and teenagers are uniquely vulnerable to these and other intrusions of their privacy in online spaces. Young people growing up in what Solove terms "Generation Google" are subject to threats against their privacy and reputations like never before, particularly since they are participating on social media at ages when they are not developmentally mature enough to gauge long-term risk or grant informed consent in the same ways as adults (Johnson, Blum, & Geidd 2009). And even if minors themselves are not engaging with the online world directly, their parents are still making choices about how their child or teenager's data and personal information is shared in cyberspace—choices that the minors may not agree with upon reaching the age of majority[1], or that may negatively affect them if uncovered via search engine or data leak (Ward 2015).

[1] In 2016, French Internet ethics experts warned parents against posting content about their children on social media due to the potential for lawsuits in the future, as France has strict privacy laws regarding "publicising intimate details of the private lives of others" without consent (Chazan 2016). The French police force also posted public service announcements warning parents to avoid memes that asked them to post personal information or photos of their children, as these can be stolen by pedophiles or identity thieves (Chazan 2016).

2.4 Privacy, Social Norms, and the Impact of Big Data

Is worrying about data privacy truly necessary? On the one hand, the aggregation of people's data allows us to enjoy greater personalization of the information we see online when we shop, travel, or read. Aggregation of health data like sleep habits or fitness levels can aid in medical breakthroughs. On the other hand, we cannot know what might happen to our data if we do not regulate the agencies that collect it, and advances in both computing and data collection have made it increasingly difficult to truly anonymize the data we spread when we go online. In "Broken Promises of Privacy: Responding the Surprising Failure of Anonymization," Paul Ohm (2010) explains the Catch-22 of data analytics: "Data can be either useful or perfectly anonymous, but never both" (pg. 1704). In order to strip a dataset of key information that can identify individuals, one also renders it useless for making correlations because most of the useful datapoints have been removed. The concept of data anonymity itself is a misnomer, Ohm argues; in the age of Big Data it is only possible to achieve de-identification. Ohm explains that the traditional "release-and-forget" method of de-identifying data, in which some information is simply pulled out of the dataset while the rest is passed on to other individuals without keeping a record of who has received which data, is no longer sufficiently secure due to the increased power of cloud computing (2010). Ohm further elaborates that "Computer scientists make one appropriately conservative assumption about outside information that regulators should [also] adopt: We cannot predict the type and amount of outside information the adversary can access. It is naïve to assume that the adversary will be unable to find the particular piece of data needed to unlock anonymized data" (pg. 1724). Essentially, we have reached the point where we must assume that every potential

adversary has access to *all* the possible information needed to reidentify a given individual or group, particularly because qualitative social media content, like blog posts, Tweets and status updates, provide extremely unique data points about those individuals that can be linked to other identifying data.

Given the ease with which many disparate points of data can be reconnected with an individual, it is important to recognize that the United States lacks comprehensive federal legislation on how collected data can be used and stored by commercial entities. For example, there is no law or policy dictating how long a company can retain data it has collected online, nor are there required conditions under which various categories of data must be deleted (Reidenberg 2014). Without such legislation, commercial entities have an increased incentive to retain consumer data ad infinitum, since finding new links between customer information means that advertisers can sell more products over time. While US law does protect against *access* to private data, these protections only extend to government actors, not to private companies. Additionally, most electronic transmissions are not protected under the Fourth Amendment because the data is transmitted by third parties and therefore technically public, implying that there is no reasonable expectation of privacy with regard to their contents (Reidenberg 2014). The Supreme Court has recognized the danger inherent in this accumulation and aggregation of data, noting in the case of *US v. Jones (2012)* that "Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes" and indicating that "aggregation of [GPS] data reflecting movements on the public street might constitute a cognizable privacy violation" (Reidenberg 2014, pg. 589).

And while the Supreme Court has thus far held that data aggregation is protected under the Fourth Amendment against *government* search and seizure, this does not protect citizens against the collection, aggregation, and use or manipulation of their data by non-government entities. The absence of legislation focused on data collection transparency or establishing limits on what kinds of data can be gathered, and for how long and by whom, are a privacy risk to all citizens.

2.5 What Privacy Protections for Minors Already Exist?

Though the United States lacks an overarching piece of privacy legislation that protects the personal data of individuals under all circumstances, the Federal Trade Commission (FTC)'s Fair Information Practice Principles (FIPPs) establish a general framework for regulating the collection of personal data. These principles, listed below, offer little in the way of prescriptive policy, and also give individuals comparatively little control over the use of their personal data:

1. Transparency: ensuring that data is not collected secretly; providing comprehensible information about how and why personal data is collected to allow users to make an informed choice
2. Choice: giving users a choice as to how their information will be used by a company or service
3. Information Review and Correction: allowing individuals the right to review and correct personal information that has been collected about them
4. Information Protection: requiring organizations to protect the quality and integrity of personal information they collect
5. Accountability: holding organizations accountable for complying with FIPPs (FTC 2000)

Minors receive several types of additional data privacy protection at the federal level, and some state and local legislatures have also added supplementary legislation. Children under 13 are granted specific protections against data collection by commercial apps, websites, and online services by the Children's Online Privacy Protection Act

(COPPA). The act, passed by Congress in 1998 and most recently amended in 2012, is enforced by the FTC and affects how commercial entities are allowed to gather information about children. The regulations dictate how companies are required to display and word their privacy policies, and outlines what kinds of data from children companies are allowed to obtain or keep (FTC 2000). In order to receive permission to use a child's personal data, the website or online service in question must obtain "verifiable" parental consent in the form of a signature, verbal assent, or credit card purchase. Different from the FTC's FIPPs, companies that collect personal data from children must also offer options for parents to request deletion of their child's data. The FTC is able to levy stiff penalties against sites or services that do not comply with the data-protection regulations; the fine for non-compliance with COPPA is currently $40,000 per violation (FTC 2016), and in 2016 several major toy companies including Viacom, Mattel, Jumpstart, and Hasbro were fined a collective $835,000 after the New York judiciary found them guilty of using PII data collected via cookies and plugins from third-party ad networks without parental consent (Newman 2016).

In addition to COPPA, all American youth ages 18 and under receive several types of privacy protection with regard to personal data collected in educational settings by schools that receive federal funding. The 1974 Family Education Rights and Privacy Act (FERPA) gives parents and students the right to access their data, and restricts the ways in which educational institutions can share it with others. Meanwhile the Protection of Pupil Rights Amendment (PPRA) offers data protection for families that participate in educational programming funded by the Department of Education, including safeguards on content related to personal beliefs and income level. The Children's Internet Protection

Act (CIPA) seeks to limit exposure to harmful visual material that children might view during internet searches at school (2000). Schools that receive federal funding must comply with the law by demonstrating that they possess filters that block obscene, pornographic, or damaging content.

2.6 Limitations of Existing Legislation

While the United States has clearly recognized that minors need additional data protection beyond the minimal recommended standards set forth in the FTC's Fair Information Practice Principles, federal legislation on the matter remains limited in scope. Solove (2017) cites FERPA as "weak" and "in grave need of an update." At present, FERPA only applies to government-affiliated data collection, and even then parents and their children lack the ability to have data removed or control the circumstances under which it is released to third parties; they only gain the right to view or correct the information that has been collected. Meanwhile COPPA, the main piece of legislation that defends children against extensive data collection by the private sector, is limited in scope due to the complexities of online interaction: the law requires compliance from commercial entities that are aimed specifically at children, but does not apply to general-audience entities unless they receive "actual knowledge" that they have collected, used, or disclosed personal information belonging to children under 13 (FTC 2013). Many social media apps popular among teens and tweens, among them Instagram, Snapchat, and Facebook, are considered general-audience platforms and explicitly state that users must be 13 and older so that they do not fall under the umbrella of COPPA's regulations. Other limitations of COPPA are that it does not require companies to disclose the length of their

data retention or for what purposes data will be used. The only disclosure requirement specified by the legislation is that parents must clearly consent to the data use policies of the given site, app, platform, or device in exchange for allowing their child access to it.

In the absence of new federal legislation, some states have begun to enact privacy laws with stronger standards to protect minors from invasive data collection by commercial entities, although only California and Delaware have passed laws that regulate both data retention and use of micro-targeted advertising with regard to minors (State Laws Related to Internet Privacy 2017). Seven other states have passed broad data protection laws that regulate privacy policy requirements, the protection of personally identifiable information, and ISP data disclosures, but data privacy legislation is currently a low priority for most states (State Laws 2017). This may change, however, due to the March 2017 Congressional decision to block FCC privacy regulations for ISPs: by April 2017 both Minnesota and Illinois had already proposed state legislation to compensate for the withdrawal of federal privacy regulations (Collins 2017).

2.7 Where Are Minors Most Vulnerable to Privacy Intrusions?

Even with data collection consent mechanisms in place, many parents are not deterred from allowing their children to use online websites or applications that gather personal data. Statistics show that large numbers of minors, even children as young as two or three years old, are engaging in regular online activity:

1. Children and teenagers are frequently left to use computers or mobile devices unsupervised. When children engage online without an adult present, there is no guarantee that informed consent to data collection is taking place, which puts the child's personal information at risk (Kessler 2011).

2. Even if they are not actively using gaming sites, apps, or social media, children and teens still acquire data footprints due to parental information-sharing decisions that the children might not have consented to if they were capable of doing so.[2]
3. Existing regulations may not be preventing as much data collection as we believe. A 2015 study by the Global Privacy Enforcement Network revealed that 67% of nearly 1,500 apps and websites targeted at or popular among children collected personal information that could be passed along to third parties; and that 71% of the sites and apps did not offer accessible means of deleting the information they collected (UK Information Commissioner's Office 2015).

In addition to concerns about data collection by websites and social media apps, the increasing prevalence of items categorized as part of "the Internet of Things" (IoT) has led to grey areas concerning privacy, especially for children:

1. Personal assistant devices like Amazon Echo, Google Home, and devices like smart TVs are not intended for use by children, but are likely to record data from children in homes that use them—Samsung's 2015 privacy policy for its Smart TV even contained a warning not to discuss sensitive or personal information in front of it because that data would be "among the data captured and transmitted to a third party through your use of Voice Recognition" (Matyszczyk 2015);
2. Wired toys that record and "interact" with children, like Hello Barbie and Woobo, explicitly collect and transmit data about the children who use them. German privacy watchdogs have issued a warning to parents not to buy Smart dolls due to concerns over the kinds of data being collected (Ng 2017). Wired video gaming systems like Xbox Live and Playstation 4 that allow for interaction with strangers also create opportunities for children to reveal identifying information and potentially make themselves the target of harassment or crimes;
3. Wearable GPS trackers for children are marketed as a safety device to give parents peace of mind, but they also provide a vast array of data to marketers about children's fitness, health, and family routines (Maslakovic 2017).

[2] For example, parents might purchase or register their children for apps and services that require disclosing personal information, including not only things like the child's age or gender but potentially also details about their education and health, such as learning disabilities or emotional difficulties, that might be protected under other collection circumstances.

The FTC (2015) has observed that IoT devices present new challenges when it comes to protecting the integrity of the Fair Information Practice Principles. While participants in their report acknowledge certain benefits of connected devices, such as vehicles with road safety sensors or Smart home appliances that increase energy efficiency, they also recognize major risks attached to the prolonged collection and aggregation of data: "[P]rivacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions" (FTC 2015, pg. ii). The expansion of data collection by everyday objects makes it even more challenging for parents to ensure that their children's lives remain private. Even if a family chooses not to purchase any of these technologies, their children are likely to encounter them in other people's homes or public spaces, where parental control over data disclosure is nonexistent.

III. LITERATURE REVIEW

3.1 The Internet: A New Frontier in Commercial Advertising

When we apply the definition of privacy as the right to be free from oversight or intrusion by others in online space, it is important to ask the following question: who are we protecting our privacy against? Most of us concern ourselves with protecting our private inner lives and activities from the prying eyes of people in our social circles, but we may not stop to consider the strangers who view our digital footprints whenever we sign up for a new platform, service, or product. And while some of these new technologies offer us benefits in exchange for our personal data, the rise of digital surveillance by content providers and third-party advertisers within the past 20 years has also presented new ethical dilemmas in the realm of privacy (Zwitter 2014).

Andrej Zwitter (2014) argues that Big Data "requires ethics to do some rethinking of its assumptions, particularly about moral agency" (pg. 1). Zwitter explains that, prior to Big Data, moral agency in the Western sense was traditionally framed as the moral responsibility of the individual, governed by free will and individualism (pg. 2). While he acknowledges that the moral and ethical difficulties related to privacy in the age of mass data collection are not new, Zwitter argues that we underestimate the ways in which data collection, and data aggregation, can impact an individual's ability to make informed decisions of their own free will. Essentially, we are overlooking the ethical implications attached to what we might consider "impersonal" data, for adults as well as children: the way Facebook "likes" are sold to marketing companies in order to hone in on specific groups of individuals, or how information scraped from Twitter can be run through

sentiment analysis in order to politically manipulate targeted groups through the use of programmed bots that make it seem like an unorthodox political position has broad support (Zwitter 2014).

When it comes to the privacy protection of minors specifically, a great deal of emphasis is placed on protecting information from people we may know, while little attention is dedicated to data collection. This has not always been the case: in *Digital Generations*, Kathryn Montgomery explains that parental, and policy-making, concerns surrounding children's vulnerabilities online were focused directly on data collection and privacy during the 1990s and the early half of the 2000s (2007, pgs. 64-78). In the mid-1990s prior to the existence of COPPA, online marketers took great advantage of the new, exciting online landscape to solicit a wealth of personal information from children looking to access games on websites like KidsCom, which was marketed as a fun, safe place for children to congregate online (Montgomery 2007, pgs. 73-74).

Data collection in this era was also enhanced by the invention of "cookies," which marketing executives embraced as a means of gathering even more detailed data about their customers. Meanwhile, privacy advocates like the nonprofit Center for Media Education (CME), the Electronic Privacy Information Center (EPIC), and Privacy International grew concerned about how, and how much, data marketers were collecting from children under the guise of games, contests, and offers of free tangible prizes like toys in exchange for personal information about the child and their family (Montgomery 2007, pg. 75-77). Amid growing pressure from these groups and others like the American Civil Liberties Union (ACLU), and press coverage about privacy risks such as identity theft, public support for data-privacy regulation grew until Congress was forced to

respond: by 1997, a Georgia Tech survey had found that 87% of Web users desired "complete control" over the data websites captured about them, and that over 71% were in favor of new legislation to protect their privacy online (FTC 1996, Caruso 1998). Public pressure due to concern over how commercial enterprises were gathering children's data ultimately led to the bipartisan passing of COPPA in 1998.

While children under 13 were protected under COPPA, teenagers were explicitly excluded after lobbying by the National Education Association, the American Library Association, the ACLU, and other civil-liberty groups. Teenagers were already excluded from other media advertising laws aimed at children (Kunkel 1988) and were legally allowed to make purchases or participate in store contests without an adult present in physical spaces, so to require adult consent online for the same activities was deemed "burdensome" to parents (Montgomery 2007, pg. 96). Advocacy groups were also concerned that teens' rights to free speech and privacy would be compromised if parental consent was required every time they went online, specifically in cases where teens might want to access sensitive information about things like birth control or abortion (Montgomery 2007, pg. 97).

Despite the broad public awareness that media and advertising exposure can be harmful to children and teens (Montgomery 2007, Livingstone, Haddon, & Gorzig 2012, Bleakley et. al 2014), and despite near-unanimous public agreement that teenagers were just as vulnerable to targeted data collection as younger children[3] in the early 2000s,

[3] A 2000 study by the Annenberg Public Policy Center found that a majority (over 60%) of parents surveyed found that parents were more worried about the disclosures their teens might make online than they were about their younger children; another portion of the study revealed that "even teenagers as old as 17 were quite willing to give up their names and addresses, along with other personal information, to

privacy and data collection all but disappear from the list of parental concerns about being online by 2005. This shift is evident in literature from the 2010s, which focuses heavily on issues of child safety online even as privacy concerns have grown in the face of increasing government data-collection surveillance initiatives like the Patriot Act (2006) and the NSA's Prism program (2013), as well scandals instigated by WikiLeaks in 2010 and 2016 (Smith, Seifert, McLoughlin & Moteff 2002; Berkman Center for Internet & Society 2002; Greenwald & MacAskill 2013; Zittrain & Sauter 2010).

3.2 Safety Over Privacy

Why, then, if the impacts of online surveillance and third-party data collection dominated public and political discourse surrounding children for an entire decade, did parents shift their focus away from privacy and instead toward safety during the mid-2000s? In her book *It's Complicated: the Social Lives of Networked Teens*, danah boyd (2014) observes that the reframing of online threats to children occurred between 2004 and 2007, specifically due to the influence of traditional media messaging on television and in print journalism (pgs. 98-112).

By late 2004, social media use among teenagers and young adults was on the rise: Facebook was well on its way to 1 million users, MySpace had over 5 million users, and blogging platforms like OpenDiary, Xanga, and LiveJournal had already gained legitimacy as ways for young audiences to share their lives with each other online

---

commercial Web sites" (Fetto 2000) and that 96% of parents surveyed believed that consent rules were also needed for teens (Fetto 2000).

Two 2016 studies, one by Ofcom and one by Stanford University, have found that children and teens still have difficulty distinguishing ads from reputable information (Stanford History Education Group 2016, pg. 10), and that they are prone to trusting information from search engines they perceive as neutral, even when that information is labeled an ad (Ofcom 2016, pg. 9).

(Facebook: 10 milestones on the way to success 2010; Stenovec 2011; Marcus 2010). Teens embraced these new spaces while their parents remained largely unaware of how they worked, at least until news stories began to break in 2005-2007 about sexual predators using MySpace to lure teenagers out of their homes (Williams 2006; Poulsen 2006). As boyd explains: "Starting in 2005, news media across the United States began to suggest that MySpace was an unsafe place for youth[. …] Although this was not the first time that the issue of online sexual predators emerged in media, previous discussions had taken place before the Internet had become mainstream among teens and before social media had become a media phenomenon" (boyd 2014 pg. 101).

According to the teens boyd interviewed between 2005-2012, parents readily absorbed these often-overstated media messages about "stranger danger" on MySpace, whether they were delivered in the form of actual news broadcasts or episodes of Dateline's *To Catch a Predator*[4], which aired from 2004-2007 (boyd 2014). boyd contextualizes this reaction by comparing it to the pre-Internet ways in which adults took out their anxieties over the safety of minors by restricting the movement and independence of children and teens, citing examples such as curfew and anti-loitering laws. These policies were enacted to reduce youth crime, but ultimately had little impact, despite the public belief that they were effective policies (boyd 2014, pgs. 103-104).

Cultural shifts, such as the emergence of new technologies or forms of media expression, often instigate anxiety about youth safety: in the past 300 years, adults have fretted over the influence of everything from printed novels to comic books, to musicians

[4] An American reality series sponsored by the television news program *Dateline NBC*, that featured hidden camera investigations in which a confederate would impersonate a young teenager looking to chat with strangers online. Adults who responded with requests to meet in person for sexual activity were arrested as part of sting operations in collaboration between the program and local police.

and television, to video games and now the Internet (Springhall 1998). Sociologist Stanley Cohen refers to these cultural moments as "moral panics," in which adults worry about the moral degradation inspired by a particular social force, often in the form of delinquency or looser expression of sexuality (Cohen 1973). When this occurs, it often contains a gendered undertone: the social and pop culture habits of girls frequently come under greater scrutiny and are more likely to be criticized or controlled (Solomon & McChesney 1993). The eruption of media attention and anxiety over MySpace in the mid-2000s reflected this trend.

3.3 Using Big Data to Decode Parent & Teen Perceptions of Privacy

As American society transitioned from the 2000s into the 2010s, the Pew Research Center's Internet & American Life project engaged in a large number of studies that used surveys to understand teen behavior online amid the rise of social media and growing concerns about cyberbullying, generating a large pool of literature about how teenagers both interact in digital spaces and protect their privacy online. The Family Online Safety Institute (FOSI) has also contributed several significant studies that use survey and focus group data to understand the ways in which parents and children approach safety and privacy concerns.

According to the Pew report by Madden et al. (2013) that examined teenage social media use, teens are not concerned about third-party acquisition and use of their personal data (which includes images and video); teens instead focus on what they believe is a more important threat: protecting their privacy from people they know in real life (pgs. 1-2). Yet while teens express fear about their data being seen by parents, peers, or school

administrators, they are still extremely likely to post publicly identifying information about themselves on various social media platforms — anywhere from 70 to 90 percent of teenagers posting their names, birth dates, school locations, areas of residence, hobbies and interests, and photos of themselves on social media accounts (Madden et al. 2013, pgs. 2-3). Teens have the impression that making an account "not public" is the same thing as keeping their data private. When asked about privacy concerns regarding the social networking site Facebook, one teen understood the privacy policy as: "Anyone who isn't friends with me cannot see anything about my profile except my name and gender. I don't believe that [Facebook] would do anything with my info" (Madden et al. 2013, pg. 10).[5] Teens also seem unaware that people may intentionally befriend them on their public or private social media accounts in order to access their personal information, as evidenced by the percent of teens surveyed who said that they or a family member had gotten into trouble with work or school due to something the child posted online (Madden et al. 2013b, pg. 75).

A similar study conducted by Hart Research Associates for the Family Online Safety Institute (FOSI, 2012) agreed that teenagers are diligent about protecting their privacy online, at least when it comes to privacy settings like restricting the audiences on their posts, blocking individuals, removing tagged photos, or marking comments as private. Different from Pew, FOSI's 2012 study also examined the behavior and attitudes of parents in addition to teens, and observed a "generation gap" between the two when it came to behaviors like online monitoring. Their survey of 500 parents and 511 children

[5] Facebook does, in fact, provide data from user profiles to third parties in order to enable targeted advertising. As of 2013, 85% of Facebook's revenue came from ads. Government agencies and potential employers also use Facebook to gain information about individuals based on their profile data (Andrewsi 2012).

found a "substantial" gap between how well teens felt their parents monitored their activity versus how much oversight parents reported: only 39% of teens said that their parents monitored their activity "very (11%) or somewhat closely (28%)," while a vast majority of parents (84%) reported that they monitor their teens' activity "very (31%) or fairly closely (53%)," and there was a similar gap between teenage and adult perceptions about how informed parents were with regard to the specifics of their children's online activities (FOSI 2012, pg. 2). The report also found a discrepancy between how well parents and children believed they were having meaningful communication about rules and expectations in online spaces. 93% of parents said they had discussed such issues with their children, while only 61% of teens agreed (FOSI 2012, pg. 4). Despite this, the FOSI study found that a large majority of both teenagers and their parents felt that teens were safe online (95% vs. 94%), although there was a slight difference with regard to gender: boys were more likely to report feeling safe online by a margin of 8%, while parents of boys reported a greater feeling of safety for their sons by a margin of 6-8% (2012, pg. 10).

With regard to data collection and privacy, the FOSI (2012) study found additional gaps between the perceptions of teens and their parents: among the concerns expressed by teenagers when it came to the implications of their data online, identity theft (44%), difficulty with college acceptance (32%), difficulty with future employment (30%), and having strangers learn who they are based on their online content (29%) were all among the top five (pg. 14). By contrast, parents believed that their children's biggest concerns included things like "someone posting an ugly or unflattering picture of me" (30%), or "friends making fun of me for an online post" (29%). Parents rated concerns about the

long-term ramifications of data collection such as difficulty with college or job acceptance, or even being tracked by companies for advertising purposes, as less important than their children did by gaps of anywhere from 10-22% (FOSI 2012, pg. 14). The only concern that teens and parents prioritized similarly was that of being contacted by a stranger.

3.4 Parents and Digital Monitoring

Further research published by FOSI in 2014 and 2015 consistently reports that parents are confident in their ability to keep track of how their children are using technology, although parents of younger children express greater confidence than those of teens (FOSI 2014; FOSI 2015). Parents of teenagers were far less likely to feel confident, but were also less likely to say that they monitor their children's technology use closely (FOSI 2014, pg. 1). Despite this, the FOSI survey data has also found that a majority of parents (over 60%) do not use any form of parental controls to restrict or monitor their children's Internet use, "because they think they are unnecessary … and because they have rules and limits in place for Internet use" (FOSI 2015, pg. 2). Most parents report having rules in place about when and how their children can get online, and what devices they are permitted to use (FOSI 2015, pg. 2). Monica Anderson's (2016) Pew study on parents, teens, and digital monitoring yielded similar results, observing that a majority of parents have done things like check their teen's social media profile or browser history, while relatively few had employed parental controls or monitoring tools (pgs. 5-6). The Pew study also found that parents of younger teens were somewhat more likely than those of older teens to engage in every kind of monitoring, and that younger parents were more

likely than older parents to know the passwords to their teen's cell phone as well as their social media accounts (pgs. 7-10).

The FOSI and Pew studies also examined how parents learned about different concerns with regard to their children's online activity, and how they subsequently addressed these concerns with their children. In FOSI's 2014 study, parents responded that they were most likely to trust advice from their children's school teachers, followed by their own children, parenting websites or magazines, and other parents (pg. 16). A majority of parents in the Pew study also reported talking to their children about appropriate conduct in their digital lives, although the study found that more-affluent parents were less likely to have regular conversations about both online and offline conduct than parents who were less affluent and less educated (Anderson 2016, pgs. 11-14). Both FOSI's (2015) and Anderson's (2016) studies also note that Hispanic parents are "especially likely" to talk with their children or teens regularly about about appropriate online behavior and media consumption habits, even though they express lower levels of confidence about managing their children's behavior or media use (FOSI 2015, pg. 18; Anderson 2016, pg. 15). FOSI's study of this difference suggests that the discrepancy may be an attempt by Hispanic parents to compensate for lower knowledge by paying greater attention.

3.5 Parents and the Internet of Things

As new devices aimed at children enter the market of IoT products, current literature offers mixed opinions toward them due to concerns over both surveillance by corporations as well technological vulnerabilities like hacking by third parties. A 2015

analysis of how children play with IoT video game figurines, like those for Disney Infinity, also suggests that "this new technology has entered many homes by stealth as parents and children were not really aware of how the technology captured children's interactions," and that many parents are not entirely aware of what IoT children's products do or how they work (Manches, Duncan, Plowman & Sabeti, 2015).

A risk assessment published in January 2016 by *Ars Technica* found that many IoT devices with cameras could be easily hacked and streamed online, baby monitors among them (Porup 2016). The assessment echoes the findings of Manches et al. with regard to consumer understanding of IoT devices, noting that "[m]ost consumers fail to appreciate the consequences of purchasing insecure IoT devices. Worse, such a quantity of insecure devices make the Internet less secure for everyone" (Porup 2016). Porup argues that federal or private regulation of such devices is necessary since they are not tested to withstand intentional attacks.

A December 2016 report issued by FOSI and the Future of Privacy Forum also called for additional legislation of IoT devices, this time specifically those marketed to children. The report concedes some of the positives that have emerged from the creation of IoT products for children: connected dolls, stuffed animals, and toy robots can offer more interactive play and engagement with creative storytelling; and connected toys "are also being used in pediatric healthcare for treatment and diagnosis, [as well as] breaking into other new settings such as education and therapy," and helping children with disabilities experience new forms of play (FOSI 2016, pg. 16). Despite these benefits, the FOSI report acknowledges heightened concerns over the privacy and security of data these connected toys collect from the children who play with them (FOSI 2016). Their

concerns are less focused on large-scale security risks, but rather recommend that toy manufacturers and app operators "maintain strong privacy policies and responsible data practices when developing, selling, and updating connected toys and services" in order to mitigate possible concerns about children's exposure to marketing while using such toys, or to minimize the possibility that toys relying on Bluetooth technology may have their data scanned by an outside party while the child is traveling through a store or an airport (FOSI 2016, pg. 12).

IV. METHODOLOGY

4.1 Approach

As discussed in the previous chapter, investigations of how parents manage their children's online lives have utilized a variety of social science research methods, including surveys, focus groups, interviews, participant observation, and textual analysis of chat logs found in various online environments. Much of this literature, however, has focused primarily on the online habits of children and teenagers, with parents treated as supplementary figures who can provide additional insight. The Family Online Safety Institute (FOSI), however, has published several studies that concentrate on parents and their feelings when it comes to supervising their children online, using a combination of online surveys and focus groups. Their 2014 report entitled "Parenting in the Digital Age" indicates that 76% of parents agree that they are concerned about data collection and tracking by advertisers, but the vast majority of the focus group and survey responses remain focused on safety rather than privacy concerns (FOSI 2014).

FOSI's 2014 survey also indicates that the most common responses parents gave to the question "Of these people and groups that could provide information about how to best maximize benefits and minimize harms of children using technology, […] which two would you trust most?" were their children's teachers (38%), followed by their own children (29%), and then by other parents (28%) (pg. 16). This correlates with responses I received during my pilot study, in which four out of six participants cited lack of parental awareness as a root cause of student behavioral issues related to technology use (Hild 2016). One administrator also noted that he had to host regular events for parents to

explain privacy-related issues, e.g. that they should not allow their elementary-age children to use social media platforms like Instagram and Snapchat since they are not required to comply with COPPA legislation regarding the collection, use, and sale of children's data (Hild 2016).

My research in this paper uses a qualitative approach to explore how well parents understand data privacy concerns as something separate from general safety concerns related to problems like cyberbullying or interaction with strangers. I conducted semi-structured interviews and demographic questionnaires with 12 parents who had at least one school-aged child (ages 5-17). I chose this age range in part because it was similar to the selection criteria used by FOSI and Pew in their survey research, but also in part because so much of the existent federal data privacy legislation related to minors is specifically focused on educational data. Some participants also had additional children whose ages fell outside these parameters, but who were occasionally mentioned by their parents as points of comparison.

4.2 Implementation

Participants were recruited using snowball sampling in order to efficiently locate parents with children in the desired age range (Bernard 2002). Recruitment began via participant referrals from parents and colleagues I have previously worked with, and expanded from that initial pool to also include referrals from participants themselves. Interviews and questionnaires were audio-recorded and took place by phone.

The demographic questionnaire at the start of the interview asked participants to provide their age, race, ethnicity, city of residence, profession, and education level, as

well as the ages, genders, and racial/ethnic identities of their children. Participants were also asked to identify what kind of school their children attended (e.g. public, private, charter, home school). Interview topics covered three major areas: participants' own familiarity with different kinds of technologies and comfort levels using them; participants' strategies for protecting their children from intrusive data collection or other online threats; participants' strategies for setting privacy and safety rules with their children; and, participants' content knowledge regarding different aspects of data privacy. Content knowledge covered topics such as their awareness of federal and state laws related to children's online behavior, their familiarity with cookies as a data-tracking technology employed on websites, their use (or lack thereof) of online tools or device features to limit data collection, and their familiarity with cyber crimes that involve privacy violations and that occur within online communities in which minors are likely to engage.

4.3 Limitations

While snowball sampling was effective for rapidly locating interested parents who met the selection criteria, racial and ethnic diversity of participants was limited based on the identities of the referrers and on the availability of those who responded. I received 22 initial "yes" responses out of 27 requests, but only 12 participants completed the interview process. A number of families were ultimately unable to participate due to school holidays or other travel, and some single parents were unable to find time to respond due to childcare demands. As a result, the demographic profile of the parents interviewed is more narrow than I would have preferred.

All 12 participants live in suburbs of large cities in the Northeast; and 10 out of 12 participants also live in communities with a median family income of $100,000 or more. Parents with limited English comprehension were excluded due to the complexity of some questions related to legal or technical terms. Additionally, due to my long association with the education profession, teacher-parents are somewhat overrepresented (3/12 participants), although this ultimately became beneficial when looking at their responses in comparison to those provided by non-teachers.

4.4 Analysis

Interviews were transcribed using pseudonyms generated from a random name list and then analyzed for themes and concepts within participants' responses using a grounded-theory approach and inductive coding (Glaser and Strauss 1967; Strauss and Corbin 1990; Bernard 2002). Major themes and concepts that emerged from the interview transcripts included *permanence* of digital data; *need for time* to monitor children's activity; *trust* that children will self-report activities or concerns; *behavior issues* with children or their friends in group chats; and *gender* as a relevant factor in online altercations or bullying.

V. PRESENTATION AND DISCUSSION OF DATA

I interviewed 12 parents of school-aged children and teens over a period of two months. Nine participants were female; three were male. The majority of participants were non-Hispanic white, highly educated, and resided in wealthy metropolitan areas in the Northeastern United States. Only one participant, Lori, lacked a college degree and lived in a community with an average family income of less than $50,000. Participants ranged in age from their late 20s to mid 50s. Some participants had children who were either too young or too old to be included in the study, although in cases with adult children the parents were still able to reference examples of issues they had encountered when the children were younger, or used their adult children as points of comparison against those who were still minors. (A table of participant demographics is included in Appendix A.)

5.1 General Trends

One of the most surprising things I noticed during the course of my interviews was that many parents I spoke to still conceive of "online" as a distinct place or series of activities separate from the rest of their children's lives. Despite the growing popularity of IoT devices, Dave, who works in online advertising, was the only parent who mentioned these kinds of products unprompted when asked about what kinds of devices the family regularly used at home — and was then paranoid that mentioning his Amazon Echo would set it off talking over his interview. With most parents, however, I had to prompt examples of devices other than computers or cellphones, otherwise the participants would

not mention that they owned IoT technologies like Fitbits, Smart TVs, or Internet-capable video game systems. Some did not even think to mention Internet-capable tablets like Kindle Fire unless specifically prompted. There was also no difference between parents of older versus younger children with regard to their awareness of IoT technologies.

Another interesting trend was that, even when explicitly asked about privacy-related concerns (e.g. "Have you ever refused to download an app or purchase a toy because of its data collection capabilities?"), many parents would shift the conversation back to safety or interpersonal concerns about their children participating on social media platforms like Instagram or Facebook. Here again Dave was unique, citing the game "Pokémon Go" as a specific example of an app he had rejected due to his belief that the app had an invasive data collection policy. Only three parents stated that they had ever decided against purchasing or downloading an app based on the kinds of data it wanted access to on their child's device. For the majority of respondents, however, "privacy" only extended as far as worries that their child would post inappropriate content online that might bring them into direct contact with strangers, or into conflict with people they knew in real life, which echoes the results of previous surveys about parents' biggest concerns regarding their children's online activity (Madden et. al, 2013; FOSI 2014).

5.2 Parental Content Knowledge About Privacy

The first half of each interview focused on assessing how much parents knew about different aspects of data privacy and what sources they relied upon to learn that information. (Questions are included in Appendix B.)

A. Cookies and Advertising

All parents had some understanding of what cookies were, although several did not realize the meaning of the term at first. Upon receiving the definition, Amy promptly responded, "Ah, yeah, I notice that on Facebook, like if I'm on the Internet [elsewhere] researching something I'll see it pop up on Facebook … in the ads, or you know, I'll see a group that pops up on a related subject." Carol also agreed that "I know that [the data tracking] happens, but I guess I didn't know it was cookies that did that."

Most other parents were aware that cookies were pieces of data that a website or advertiser used to learn information about what they viewed or clicked on when visiting any given site. Dave, however, grew amused at the question, explaining that "[my job] is to come up with cookies that will collect specific kinds of data for different clients." He gave the most detailed definition of what cookies are, and how they work, sharing that they do not only identify your device or collect information about browsing history but also:

> *in some cases … they allow you to scrape data off of various fields when you're filling out forms and things like that … and send them back to whoever owns the cookie. Or in some cases you can use the cookie to identify data that's been scraped elsewhere, so it's a combination of the two. It will know this cookie, which attaches to this browser, which attaches to this device. [... And] it's not just cookies. It's about identity. So, how many different ways can I identify the same person so I know it's the same individual or household that is using multiple devices? … and then ultimately you want to tie it back to a true identity link: an email address, a postal ID, an address, a phone number."*

Dave laughed, and then added, "I just want to know who they are. And what they like, what's their lifestyle like, and what interests do they have. What are their demographics and any other psychographic information that I can get my hands on or infer from their browsing history, their app behavior, things like that.

Dave was also one of few parents who used a cookie-tracking browser extension (Ghostery), although he explained that he doesn't use it in the way someone concerned about privacy might: "I need to know from a competitive standpoint who's using a site, who's looking at it, since maybe these are companies I should reach out to." For him, cookie-tracking is a tool that helps him identify who is gathering data from any given site, not a tool he uses to block cookies or ads. He pointed out that agreeing to use a browser extension to block ads is still a data tradeoff anyway, noting that "no matter what you do, you're always exchanging some data from yourself and giving it to somebody else in exchange for something else."

The only other parent who said yes regarding cookie or ad-blocking tools was Sara, who works in data analytics, and this was because "my husband is also an IT professional and very good about making sure the computers are updated for all of that." Amy and Jennifer offered "maybe" responses, for similar reasons: both said that it was possible their husbands had installed a browser extension to block ads, but that they didn't know for sure. Of the parents who said no, Brian, who works in cybersecurity, explained that "I just didn't batten down the hatches to that level" despite having a good understanding of how cookies worked.

More parents were aware of how to turn on ad-blocking or reset the advertising ID on their mobile devices, with four out of 12 saying that they had done so. Amy noted that she "[goes] through those settings as much as I can" since they are more accessible than the settings on a computer. Sara, who did not know where to find those options, actually paused our interview in order to ask me

where to locate them on her iPhone, observing that, “Even though I am in information technology and I work with computers all the time, I still don’t know these things. I feel like a whole lot of people aren't aware of these things.”

B. Malicious Data Theft

In order to gauge whether or not parents had come across any media that focused specifically on privacy issues, I asked them whether or not they had ever encountered the words doxxing (in which malicious actors research and broadcast private or personally identifiable information about their target) or swatting (in which malicious actors not only obtain their target’s address but also deceive law enforcement officials by alleging that their target has committed a serious crime). Both kinds of attack are used to harass or harm others, and have been perpetrated by/against teenagers in several major cases within the past two years.

Only two participants, Jennifer and Denise had heard of doxxing, although Denise was only familiar with the practice, not the term. None of the participants had ever heard of swatting even though it made national news last year after a teenage boy who was the star of a popular Internet meme became the victim of the practice (Lewis 2016).

C. Internet of Things

The majority of participants had never encountered this term. Only Susan, Dave, and Brian knew what it meant, with Brian explaining, “It implies that they’re putting Internet in lots of devices in your household that years ago would

just be their own little thing: your thermostat, your television set, your refrigerator. It's the life that is on the Internet."

D. Data Privacy Legislation

About half of the participants recognized COPPA, although most had only a vague recollection of encountering it. The ages of participants' children did not seem to affect who knew about it, although the two participants who provided clear examples of how COPPA applied to them did have multiple children under age 13. Lori recounted that her elementary school-aged daughter had wanted to play a game called "Animal Jam" that required her to register and consent to the privacy policy in order to allow her daughter to play. Pam referenced several occasions when she'd provided consent for online games like Club Penguin and academic sites like Khan Academy. However, Pam also mentioned that she had already heard of COPPA before her children started using these sites, because:

> *I received a mass email from the elementary school principal with the subject header 'Instagram: Should your child have it?' when my oldest [son] was in fifth grade. … [The principal] reminded us that children are not protected under [COPPA] if they sign up for accounts like Instagram before age 13. I'm not sure how commonplace that is, and I actually agree with him, but it infuriated a lot of parents.*

Compared to COPPA, parents were far less aware of other types of data privacy laws, with zero having any idea whether their states provided additional legislation related to data collection, cyberbullying, online harassment, or sexting between minors. 11 out of 12 had also never heard of FERPA, with only Pam recognizing that some of the consent forms sent home from her children's school mentioned the law: "It's covered in the Internet Use Agreement Policy that is in our opening day packet at the beginning of every school year."

E. Technology at School

The majority of parents said that they had signed some kind of Internet use or behavior policy sent home by their children's schools. Susan said no, since her daughters are home schooled; while Denise quipped that "our district has too many other problems. Not terrible ones, but we're not really paying attention to technology right now."

Of those who were aware of the policies set out by their children's schools, there were differing levels of familiarity. Sara confessed that "I feel like it's there, but I haven't read it. I think there are some things that you assume are understood about how kids should behave with the Internet." Amy, who is a teacher herself, explained that she knows more detail about what the policies are and how different technology is used at her daughter's school "because I'm entrenched in the school system, so I have a better idea then I think the average parent does because I'm using them." Mark, who is also a teacher, said that "I basically go right down to the computer lab, and you can see what they use in class," although he was not sure what other kinds of computer skills might be taught by the librarian, for example. Laura, meanwhile, noted that she not only had to read and sign off on the policy at her son's school, but also had to "go to a workshop about it" because her son had been issued a laptop starting in sixth grade. She explained that the students' web use is monitored and that the computers can be taken away if there is any inappropriate use.

5.3 Parental Implementation of Knowledge with Children

A. Device Access

All participants allowed their children to use at least one form of digital device that was owned exclusively by the child. Not all parents, however, gave their children Internet access with these devices; parents of young children, like Jennifer and Denise, explained that they heavily restricted their children's use of their tablets. Jennifer said that she opted to buy a Kindle Fire for each of her elementary school-aged children because "everything included cost about $50 apiece, so if they break or drop them it doesn't matter so much," and that "I have all the connectivity settings turned off. I preload apps for them and then that's it." Denise, who is a parent of elementary school-aged twins, said that her children don't spend a lot of time on connected devices because "being a psychologist … I'm aware of brain research that suggests screen time is not the best, and just I'm much more of an outdoor person and I'd rather they do that." Her girls have one tablet that they share, but, "we have extreme rules. They don't even remember that we have it. They have no access to it other than on long drives or train rides."

Nearly all parents of tween and teenage children said that their children owned mobile phones. Most older children also owned a laptop, and about half of children also had access to connected video game systems like Xbox Live. Many participants described mobile phones as a "rite of passage" or a "necessity," and often cited the transition to middle school as the point at which they allowed their children to have their own devices. Carol and Mark both mentioned logistical and

safety concerns when explaining why their children received phones at that age, with Carol explaining that her son received his first phone "when he started walking to and from school by himself — but it wasn't a smartphone." Mark said that since his children go to middle and high school in different towns, phones were a necessity in order to keep track of all their activities.

B. Rules About Use

Susan's teenage daughters are allowed to take their phones and laptops wherever they want in the house, although she has had to impose rules on her younger daughter because "otherwise she'd stay up all night on her phone." Susan explained that she didn't have to do this with her older daughter; the younger one just had a different sort of personality and was not as good about managing her time. When it came to rules about what sort of apps the girls could download, Susan's main rule was that her kids needed to ask first. "We have a family account to keep track of the downloads." Susan said that she has also refused to let her children download specific apps based on the data permissions the apps requested.

Jennifer was less concerned with specific rules for her daughters since they are in early elementary school. "They're kind of illiterate? It's kind of hard [for them] to search for things. [My youngest] can't even type!" She said that her children occasionally use the family computer, while supervised, to watch videos or play educational games, but that for the most part she doesn't worry too much — although she does have rules in mind for the future. "Middle school is definitely the benchmark for a phone. And part of that's because it's a different

school and you need to coordinate all their activities and track them, what they're going and playing and doing."

Carol's older son has access to a variety of devices, including a smartphone, laptop, online video games, and Smart TV, while her younger son has an iPad and also navigates around on the TV. She has stricter rules about device supervision and storage: all of her children's devices must go in the kitchen at night for charging, and with her older son who has a mobile device, she tries to supervise what his activity. She explained that he's mostly on Snapchat with his friends and it's "hard to monitor that," because messages sent through the app are temporary. When downloading apps, her older son does have to ask for approval beforehand, but "there aren't a lot of apps that he wants. He's still pretty ... I don't want to say a novice, but he has his few apps he likes and that's it. But to be honest, if it was free I think he wouldn't ask, he'd just download it." With her younger son, Carol has access to his device and the apps, so she is not concerned about that what he's doing when he uses the device.

Laura's major rules are that her son isn't allowed to bring his iPad to school, though he is allowed to bring his school laptop home since "many assignments are right on the computer." Her son is less interested in his phone than in video games or other devices, though Laura said she tries to keep track of how often he's using them. "when he's at his friend's house it's harder to control cause I'm not there...I try not to let him stay on for extended hours." Laura noted that her attitude about restrictions and supervision has relaxed over time, and that she doesn't entirely know what kind of apps or social media services her son uses

online. She will sometimes take away her son's phone if "he forgets to do his homework, or if he's rude to me, or whatever."

When asked whether he gives his children any rules regarding their technology, Mark replied, "No, not really. I really don't put restrictions on them, I basically trust them. And they know that if they were to do something wrong on there and I found out, I'd take everything away from them. It's a one-shot deal. That's it. And they know, they don't hide anything. My wife has access to everything they do; she goes on their phones, she has all their passwords so there isn't anything that can be hidden." He also explained that he and his wife both receive notifications about their children's texts and group chats on their own devices. "My wife keeps tabs on what they're doing because she understands it a heck of a lot more than I do. But we all share the Apple ID, so I get the pop-ups once in a while. I don't read them all the time, but if there's ever a suspicion I can. The kids have never really noticed it, and I don't say anything."

Amy said that her family's rules about technology "did evolve naturally. I think we sat down when we laid out the ground rules, like 'if we want to look at your phone, we're paying for it so we have every right to look at it'. So when they were a lot younger we really monitored it." She recounted that her son went behind her back as a middle-schooler and started a Facebook page without permission: "[W]hen I found out I got very upset, but once I started figuring things out about how it works I was much better, because he showed us how he did the privacy settings. And that was more of a concern, the privacy and who was seeing what they were posting, versus everything else." Amy's younger teenage daughter

has her own laptop and phone, and is allowed to use multiple social media platforms. Amy hasn't felt the need to to make any of her own accounts just to keep up, although she conceded that she takes advantage of an Instagram account that she supervises for her daughter's church youth group:

> *I can check everything that goes on there, and it's interesting, it's actually very very helpful, because then anybody who follows it, I can see a lot of the kids' activities. So sometimes parents will come to me asking if their kids are on there a lot, or what I see. I haven't had to do that too much, but I know for some of the kids I have to remind them that they're representing their church … I don't think that kids realize that everything they post, everybody sees. I don't think they even take into consideration that what they post or when they comment, you can see it. And I had to talk to a couple of kids, and remind them that you have to be careful. And they were appreciative, none of them were like 'why are you looking at this.' But especially the comments, because you have to decipher the language because a lot of that stuff stands for things, and I don't know what that is. The slang and stuff changes really fast!*

Amy also said that there are no set rules for her daughter now, but that when her kids were younger they were required to plug in their phones at her desk every night, away from their bedrooms. She said she had to change those rules as her children aged, especially since they started regularly using their phones to collaborate with classmates on homework.

Brian, as a cybersecurity expert, took a very different approach than most other participants in this study: "I installed control software" on the PC his older sons used, but admitted that "it started to freak them out because they knew that Dad was literally watching." The software Brian had installed for his sons was by his own admission "intrusive": it wasn't set up to block their access to any content, but it would snapshot their activity and send it to him if they searched for any of the keywords he had flagged. He said he only ever used it to confront one of his sons once, and that "it made them feel like they were being spied on, so I disabled it when they were in high school," although he noted with amusement that the

software *did* once catch a housekeeper using the family's computer without permission. "So, because of their reaction, I took a different approach with my youngest. She got lucky. She also got to have a phone much sooner than the boys, and we had rules about keeping it downstairs the first year, but then maybe we got lazy. But she still puts it into Do Not Disturb mode and she'll use it for an alarm clock, or even to communicate with us in the middle of the night if she's awake not feeling well."

Denise hasn't set many rules for her girls, mostly because they're young and she doesn't let them use connected devices often. "We don't really talk about privacy or any of that. They don't understand what a digital space is. They've never really been in one. But we probably should at some point!" She also explained that since she is divorced, "it could be that they [are using connected devices] with their dad and I'm just not aware," but that in her house "it's like a special treat. They really only get to play with their tablet three or four times a year."

Lori has two elementary school-aged children, as well as one toddler, and while she has told her children that they have to let her check their devices whenever she asks, she mostly lets them "do their own thing." As far as monitoring, she said that her approach is just to "come up to them and ask what they're doing. It's not an issue right now, but that might change once they're teens." As far as different kinds of access to devices or apps, "I base it on what's age-appropriate," although she added that she'd wait longer before allowing her children to have email accounts because she doesn't see any need for them to have

them before high school. With regard to data privacy and app usage, Lori said she has blocked her children from downloading apps on their own and that she also checks out any apps they request first in order to decide if they're age-appropriate. And while she has turned down some apps that ask for excessive permissions, she said that she does let her children play Pokémon Go despite its geotracking, because "I used to watch Pokémon and I didn't see anything wrong with it, it's a cool game. They really only play it in the car when we're going somewhere."

Sara's family didn't really do rules with their two sons. "We tried to in middle school, when my oldest son was looking at sites he shouldn't be looking at. But I feel like he wouldn't listen, because we told him it was something he shouldn't be doing. But he was quite mature for his age, he said he knew what he was doing!" She added that she has tried to limit the amount of hours her sons spend online, especially on video games, but that ultimately she and her husband never purchased any software to control it. "Now they're at that age where they know, and they're good kids and their grades are doing fine, so we don't monitor them much. They're old enough to decide what's right or wrong on their own."

Dave's pre-teen children each have one device: his daughter has an iPhone, and his son has an iPad. "The phone has to stay downstairs at night, and we have a rule that if we ask to check it she has to give it to us, at any time. During the week I think we're pretty good at limiting how much they're on the devices," he said, at which point his wife made a sound of disagreement in the background of the interview, " … but the weekends are more lax." He added that they limit their children's access to apps and that they always ask before trying to download

anything. He also explained that, due to his own knowledge of advertising and data-tracking, he does not allow his children to create user accounts in their own names for any reason.

All of Pam's children have their own devices, and the family has rules about when or where they can use them. "They're not allowed to bring them to the dinner table, or to have them out at the table in restaurants, though I do confess that when we were dining out one night with my youngest, and she was three at the time and behaving like a three-year-old, I handed her my phone to scroll through photos while we waited for our food." Pam admitted that she feels like she relented too early in allowing her older children to have their own phones, but said that she did it "in part because [my daughter] had increasingly been texting me from our sitter's phone, which felt sort of unfair to the babysitter … and I do enjoy being able to quietly 'talk' to my children when I need to at work thanks to messaging."

C. Long-Term Effects of Digital Presence

Parents had mixed reactions when asked if they have thought about the long-range effects data collection may have on their children. Some, like Dave, said no. "At the end of the day they're going to have [a digital footprint] … eventually. We all do. It doesn't really have any bearing on whether or not they use different things. And even if we don't let them use anything, it's unavoidable because they're required to take their state tests for school on a computer." Pam had a similar outlook, noting that, "I was concerned about privacy, for myself,

when things like Facebook were a new thing. Now I worry much less about this, though I do have my own personal rules about what I will share about [my kids] online — I won't use their names in blog posts for my job, for example."

Other parents, like Sara, said they hadn't thought about it. But about half said that they are concerned. Amy, for example, said that she has worried about "identity theft, and then just people knowing too much information about them." Brian stressed a theme that was echoed by multiple other parents, noting that he is concerned because "anything you say is out there forever, literally. There are things I posted when I was first engaged and interested in places to go on a honeymoon, and this is going back to 1989, 1990, and things I asked back in the infancy of the Internet are still there." Denise also mentioned concern about permanence, but focusing it more specifically on her own sharing of her children's data, "especially since I ended up having a transgender child. I wouldn't be able to predict that, but it makes me reconsider things I shared about them when they were small."

D. Handling Disagreements about Information-Sharing

When asked whether or not they've run into a problem with a family member, friend, or child's friend sharing private information against their wishes, over two thirds of all participants said that they'd never had an issue. And the three parents who said that yes, they'd experienced a situation where there was a disagreement about information sharing, also said that it was easy to address those situations when they occurred. In Amy's case, she and her son had disagreed about

a photo collage she posted for his birthday: she thought it was cute, he was embarrassed and didn't want his friends to tease him. Sara said that her older son ran into a problem in high school where a classmate posted party photos online that were not appropriate and included him. As to how she and her son resolved it? "I told him, you have to call the person right now and tell him to take down those pictures, and he did take them down." Dave also ran into a situation where some family friends reshared a photo of his son that he ended up asking them to delete: "It wasn't malicious, they were trying to help him accomplish a school project. Everyone was really understanding about it."

E. Advice Given about Online Behavior

The majority of parents have addressed situations like talking to strangers or dealing with negative behavior from peers, although they acknowledged that their children rarely encountered either problem. A common piece of advice, as articulated by Mark, was, "Don't give out any information online. If anybody tries to contact you, don't answer, bring it to us right away." Jennifer used a lighter sense of humor when advising her young children: "I definitely tell them, 'never take a naked picture!' … I'm mostly concerned about them making bad choices." Lori offered similar advice, although a little more seriously, explaining that she often tells her daughter, "If you put a picture on social media, it's going to be there forever, even if you delete it," because other copies of it might linger in cloud storage or on someone else's hard drive. Lori also said that she tells her daughter "not to let people take pictures of your body or anything you feel uncomfortable

with." Susan, whose daughters are both dancers, has run into a unique situation with online behavior in addition to the usual concerns about oversharing: "We've learned, with Instagram, that the girls have to be really careful what they share from the studio, because sometimes the choreography is copyrighted and they've been asked to take the videos down."

5.4 Discussion of Themes

One of the most consistent themes that appeared in the parents' responses was that of *permanence*: two-thirds of all participants explicitly mentioned words like "permanent," "forever," and "always out there" when discussing their major concerns about their children's behavior online. Yet, while parents say they are worried about the content their children might potentially post in the future, most focused specifically on the idea that their child might post an embarrassing or regrettable photo online without elaborating on what the consequences for such an action might be. Only two parents articulated reasons why the idea of their children accumulating long-term digital footprints might be a problem. Amy mentioned that she had worried about how her son's online data might harm college acceptance chances, because "you hear stories about how colleges may look through your Facebook page and whatever." Denise also said that she was concerned about the broader consequences of her children's online presence, even though they're still young, but for very different reasons:

> *One thing that I ... I don't know if this is a privacy thing, but I would be worried about [my transgender daughter] being trolled, or seeing comments about transgender people, or having comments like that directed towards her. I also worry, and this is kind of paranoid, but especially with the Trump administration now, I'm not sure how safe it is to have a trail of data that says you're transgender. I don't know if that's avoidable, but I have concerns about that and I think it's ... not likely, but there's some chance that someone would target her in person because they found her or found out about her online.*

Additional issues related to gender were a theme that occurred regularly, although often in more subtle ways than the concerns Denise expressed about trans identity. Three different parents — Lori, Dave, and Pam — mentioned that they had greater concerns about their daughters online than their sons, and all three brought up worries about how the image-driven nature of social media culture might affect the confidence and self-image of their female children as they grow older. All three parents also explicitly mentioned "meanness" by girls as a justification for their concerns, with Lori remarking that "With my son, [I don't] really worry? Being a girl is a little tougher," and Pam sharing an anecdote about a time she caught her middle-school daughter playing the "elimination game" on Instagram, in which her daughter and classmates posted a grid of their peers' photos and then voted them out one at a time until only one remained. "I talked to a friend with a slightly older daughter, and in her circles the elimination game was clearly a beauty contest. I didn't like where this could potentially go."

Despite these concerns raised by parents of girls in my participant group, other parents like Susan reported that they never ran into any problems with their daughters; indeed, parents of boys were the only participants who shared that their children had been involved in online "drama" or bullying, at both the middle and high school levels. Carol disclosed that her son had been involved in an incident with another boy in his grade who was sending vulgar text messages to classmates, although he was "more on the outskirts of it … [until] the end of the school year. And it wasn't as bad as [what happened to]

some of the other kids — he was sort of a bystander because he was a witness to something this bully did, and the parents of the other boy knew this." Amy recounted that her son had been involved in more online conflicts as a high school student than her daughter, including an incident in which he was accused of storing inappropriate photos on his phone: "I had access to his account, and I told the family that I hadn't seen anything, and my son swore he didn't do it. It eventually turned out that the girl was the one spreading inappropriate photos, but it was a mess. But [my son] was very honest about it [with us]."

Honesty and trust were also brought up frequently by about half of the participants, particularly those of older children, and were also associated with how closely parents chose to monitor their children's activity on their devices. Parents like Mark or Sara, who explicitly said that they trusted their children to make good choices and talk to them if there was a problem, also admitted that they were more lax about keeping a close eye on everything their children did online.

In addition to values like honesty or trust, some parents mentioned that lack of time affected how thoroughly they monitored their children's activity. Mark, Amy, Brian, and Sara all agreed that it was "too much work" to constantly sift through all their children's messages, emails, and other activity in addition to keeping up with their own.

5.5 Additional Observations

My results appear to support existing survey data regarding differences in monitoring style based on ethnicity, income level, and education (FOSI 2015; Anderson 2016). White, wealthy, and highly-educated parents, particularly those of teens and pre-

teens, showed the least awareness when it came to data collection and privacy concerns; and those who had younger children, like Jennifer and Denise, largely assumed they did not need to think about data privacy issues because their children were not actively using the Internet. By contrast, Lori, a Hispanic working-class parent, demonstrated some of the greatest awareness of privacy laws like COPPA, and also mentioned a number of detailed conversations she has had with her children about online privacy and safety even though they are only in elementary school, which suggests that there are underlying cultural differences at play. Additionally, only two parents, both of whom were members of minority ethnic groups, recognized that the interview question about teaching children "how to protect data from police or other law enforcement agencies" was in fact a differential question meant to capture parental priorities based on race or ethnicity.

The responses of teacher-parents and non-teacher parents did not differ greatly with regard to how parents educated themselves about privacy and safety concerns that affected their children. Teachers were just as likely to say that they consulted friends when seeking information about an app or site their children were interested in, and were no more likely to know about COPPA, FERPA, or state data privacy regulations than the rest of their peers. The one major difference that came up was that teachers were more likely to know a) if their children's schools had a digital use policy; b) what kinds of hardware and software their children were using through school. This is striking given that FOSI's 2014 report on parenting in the Digital Age revealed that parents consider their children's teachers their most trustworthy source of information when it comes to online safety and privacy issues.

My results also appear to support some of the concerns raised by FOSI's 2012 report on the digital "generation gap," in that the parents I interviewed did not seem concerned by, or even aware of, safety issues presented by many platforms or app services that their teens and tweens might be using, let alone how those might also be gathering data about their children and sharing it with third parties. While parents like Susan, who homeschools her children and subsequently spends a great deal of time around them, and Pam, who works with a parenting magazine, both mentioned that they were familiar with the concept of the "Finsta" versus the "Rinsta" (Fake vs. Real Instagram; the former is open to the public while the latter is reserved for close friends and family) as a way that teenagers mediate their social media presence, no other parents of teens or tweens brought it up. Most parents also did not mention Messenger as a service separate from the Facebook platform, nor did they acknowledge that both Facebook and Instagram also offer livestreaming video – in fact, when informed of this one parent responded, "I hope my son doesn't do that." Parents limited the scope of their privacy concerns to the inappropriate sharing of photos, and generally assumed their children were honest with them, even though two admitted that they had caught their children using social media accounts without permission and another mentioned that his daughter had hidden a forbidden app in a secret folder on her phone.

Additionally, several parents said that they liked Snapchat as a platform their children used, even though it was harder to supervise, because the messages sent through the app were temporary and because they believed the app was a casual entertainment activity; Mark, for example, knew it as "the app with the silly faces." This was yet another demonstration of the gap in understanding about data privacy. Parents did not

recognize that, on Snapchat, their children were playing with augmented reality filters that collect and interpret data about their faces. A 2016 video investigation of Snapchat's facial recognition software by *Vox* suggested that "Snapchat sees a revenue opportunity here. In a world that's flooded with advertisements, maybe the best hope that brands have to get us to look at their ads is to put them on our faces" (Fong & Lee 2016). The *Vox* investigation concluded with a warning about the unregulated use of facial recognition data by both private corporations and the federal government that echoes the ethical concerns of both Georgetown Law's 2016 Center on Privacy and Technology report, "The Perpetual Lineup," and by Zwitter (2014), who warns that collection of such data can be used to manipulate the behavior of those who unwittingly provided it, whether that means enticing them to buy a certain product or priming them to behave a certain way by offering a particular good or service they may want (pg. 4). While this is of concern to all citizens, children are more vulnerable to this kind of manipulation than adults (Wilcox, Kunkel, Cantor, Dowrick, Linn & Palmer 2004), and taking such targeted advertising or tracking into children's private spaces via embedding them into apps or toys violates our cultural expectation that parents have the final say in what kinds of information or values they will permit strangers to share with their children.

VI. AREAS FOR FUTURE RESEARCH AND CONCLUSION

6.1 Areas for Future Research

1. Responses from minority participants indicate that there may be sociopolitical reasons why parents from low-income or marginalized groups, like members of the LGBT community or immigrant families, are more invested in learning about privacy and security issues than their counterparts in more privileged communities. Previous survey literature has not, for example, considered sexual orientation or gender identity of either parents or children as a factor in how individuals behave or protect themselves online. There is also no literature exploring whether or not non-immigrant visa holders, legal permanent residents, and/or illegal immigrants have a differing level of data privacy awareness as compared against US citizens.
2. Most parents interviewed, even those who work in IT and cybersecurity, revealed that they rely on close ties to friends or colleagues when they want to learn about online concerns that affect their children rather than consulting technology or privacy-specific resources. Further research in how to effectively reach parents with important information about data privacy and safety concerns may be beneficial.
3. More research is needed on parental awareness of IoT devices, both in general and for children specifically. Most participants had difficulty identifying their own IoT devices even when asked specifically to name them. Many parents also admitted that it had never occurred to them to ask other parents what kind of IoT devices they might have in their homes, but several said that they would consider it for the future.
4. The results of this study suggest that there may be some gender stereotyping occurring on the part of parents with regard to how often female versus male children get into behavioral altercations with their peers in digital space.

6.2 Conclusion

Based on the responses of my participants, parents have an insufficient understanding of the differences between a data privacy concern, an interpersonal privacy concern, and a safety concern. Even teacher-parents, who are presumed by their peers to be more knowledgeable when it comes to minimizing harm online, did not appear to have greater awareness than other parents, including those who had careers in IT-related fields. Parents did, however, recognize that there is a permanence to online activity that does not exist with more traditional forms of expression, and are concerned about how that will affect their children over time.

Despite this awareness of permanency, parents are still primarily focused on immediate threats to their children's safety or on the sort-term social consequences of impulsive behavior. Those who took a more reflective look at the consequences of long-term data accumulation often applied this in personal contexts, such as thinking in terms of reputation management for a child applying to college. Only one parent, that of a transgender child, mentioned concrete long-term concerns related to the accumulation of data, citing a fear that her child might be profiled or harmed in the future by either the government or individuals who are able to identify her based upon her online data. The majority of parents, however, appear to either be content with the tradeoff of data privacy in exchange for online services, or else they do not recognize that data collection may have long-term social and economic impacts on their children. For example: parents and their children have some control over whether or not a college can view their child's social media content when making an admissions decision. Parents and children do *not* have control, however, over whether or not a college may obtain access to a decade's

worth of information about their child's intellect or abilities that has been aggregated across everything from literacy games like Spelling City to language-learning apps like DuoLingo, to detailed analysis of their work on Google Classroom or reports about how thoroughly they engage with e-reading assignments via software like CourseSmart (Morozov 2012). Based on the participant responses, parents are not even thinking in these terms, let alone taking action against this kind of encroachment on their children's privacy rights.

Beyond even the pressing concerns about our children's educational futures, there is also room for additional types of discrimination that are presently unregulated. Children and teenagers who grow up in the Digital Age may be excluded from future employment opportunities because they are deemed inappropriate audiences for targeted job-seeking ads. Employment law protects against discrimination on the grounds of things like race, sex, national origin, religion, and physical disability (Discrimination by Type, n.d.); but there are no regulations about whether or not employers can buy that data from third parties and use it to limit their applicant pools before the hiring process even begins. Digital data collected from minors may also affect their future eligibility for products like health care or auto insurance based on the aggregation of information about their behavior that they've revealed elsewhere; and Big Data has already been used in cities like Los Angeles for "predictive policing" (Zwitter 2014). The potential to monitor, profile, and control individuals or communities grows exponentially when data analytics companies can look at our behavior and interests starting from the earliest years of our lives. Without greater awareness and regulation of how data is shared and stored, abuse of this potential is likely.

Existing federal and state legislation surrounding data collection for minors is not sufficient to protect against these long-term concerns. While COPPA excludes teenagers from its consent requirement for valid reasons, teenagers are still impacted by the effects of data collection and targeted marketing in ways that may lead them to make poor decisions. States like California have taken some steps in the right direction by limiting the categories of products that can be targeted to teens and by offering teens the option to request that their data be removed from any online site or platform, but these measures still do not address the problem of data aggregation or data resale over long periods of time. As Dave explained in his interview, advertisers "want to know who [you] are." In our present digital landscape, a one-time exchange of data for service is no longer a private exchange between two parties, nor is it temporary. Collect the thousands of data points spawned over the lifetime of a single mobile device or computer that can be linked to an individual and it is possible, without regulation, to develop an intimate picture of who that person is and use that information to manipulate their behavior, whether their name is known or not. Future state and federal policy needs to address the problem of indefinite retention of data, and not just within specific policy areas like health or education. Due to the spread of IoT devices and the ways we share personal on third-party platforms, nearly any service or app can collect personal data that is considered private in other, more traditional contexts. Adopting comprehensive data privacy legislation is the only way to protect against potential privacy violations in the future.

APPENDIX A: PARTICIPANT DEMOGRAPHIC TABLE

	Parent	*Gender*	*Age*	*Race/ethnicity*	*Education level*	*Occupation*	*# of children*	*# children per gender, by age bracket*				
								< 5	*5-9*	*10-13*	*14-17*	*18+*
1	Susan	F	late 40s	white	Master's	stay-at-home parent	4			1-f	1-f	*2-m*
2	Jennifer	F	early 30s	white/Jewish	Doctorate	dentist	2		2 - f			
3	Carol	F	late 30s	white	Bachelor's	stay-at-home parent	2		1 -m	1-m		
4	Laura	F	mid 50s	white	Master's	teacher	1				1-m	
5	Mark	M	mid 50s	white	Master's	teacher	4			1-f	1-m	*2-f*
6	Amy	F	early 50s	white	Master's	teacher	3				1-f	*1-f, 1-m*
7	Brian	M	late 40s	white/Jewish	Master's	cybersecurity specialist	3			1-f		*2-m*
8	Denise	F	late 30s	white	Doctorate	counseling	2		2-f			
9	Lori	F	late 20s	Hispanic	GED	stay-at-home parent	3	*1-m*	1-m	1-f		
10	Sara	F	mid 40s	South Asian	Master's	data analyst	2				1-m	*1-m*
11	Dave	M	mid 40s	white	Bachelor's	advertising manager	2		1-m	1-f		
12	Pam	F	mid 40s	white	Bachelor's	editor	3		1-f	1-f	1-m	

APPENDIX B: INTERVIEW QUESTIONS

Demographic Questionnaire

- What is your current job/what industry do you work in?
- What's the highest level of education you've completed?
- If you're comfortable sharing, how old are you? (an approximation like "mid-40s" is okay)
- What race(s) and/or ethnic heritage(s) apply to your family?
- How many children do you have? How old are they? What gender is each child?
- What kind of school do your children attend? (public, private, homeschool, etc.)

Content Knowledge

- Regarding your own technology use: what kinds of devices do you use in your day to day routines? Are there any particular apps or services you're partial to?
- How comfortable are you solving your own technical issues? For example, are you familiar with how to adjust the different settings on your devices? Do you ever look up tutorials on a website like WikiHow or watch a help video on YouTube? Set up appointments with a help service at BestBuy/Apple Store? Ask your kids for help?
- As you may know, we all leave information behind whenever we go online. Some of this is information you personally provide (like typing your address on an order form), but some of your data is tracked in ways you may not be able to control, either by your web browser or by the sites you visit and their advertising partners.
    - Do you know what "cookies" are? What about how they work?
    - Have you ever installed a browser extension to limit the amount of data that is collected about you online?
    - Do you know how to limit or reset the advertising identifiers on your mobile device?
- Have you ever heard of the terms "doxxing" or "swatting"?
- What about the term "Internet of Things"?
- Regarding your child's digital activity, how do you find out about privacy or safety concerns that might affect them? (Examples: books, newspapers/magazines, radio & podcasts, tv news, google, parenting blogs or newsletters)
- Have you ever heard of:
    - the Children's Online Privacy Protection Act (COPPA)?
        - If yes, do you remember where you first heard about it?
        - If you are familiar with it, do you understand what it means when a digital service aimed at children asks for "verifiable consent" from you?
    - State law regarding children's privacy?

- Have you ever received a digital use/behavior policy notification from your child's school?
    - Can you give examples of the kinds of technology and/or apps your child uses while at school?
    - Have you ever met with a school official to discuss how technology is used in your child's classroom? (e.g. during Back-to-School night or a parent conference; at a PTA meeting or other event with a principal, or counselor; at a Board of Education meeting)
    - Have you ever been informed by your child's school about the Family Education Rights & Privacy Act (FERPA) and/or Children's Internet Protection Act (CIPA), and what rights you have to control your child's digital information?

Implementation of Knowledge

- Do you allow your child to use any digital devices? If so, what are they?
- Do any of these devices belong exclusively to your child? If so, where are they kept? How do you monitor their use throughout the day or the week?
- Do you keep track of what kind of apps or games your child downloads, or what kinds of sites they visit or content they share on their personal devices? If so, how?
    - Have you ever refused to allow your child to use an app, toy, or other service because of its data collection policy?
    - Are you concerned about the long-term consequences of allowing your child to use digital services that collect information about their personality and habits?
        - If yes, have you considered any ways to minimize your child's digital footprint? Has your stance changed as your child has aged?
- Do you have any rules about how old your child must be in order to use different kinds of technology independently? (e.g. web search; email; social media platform) Why?
- What are your major concerns regarding your child's actions and interactions in digital space? Have you encountered any difficulties when it comes to supervising your child's digital behavior?
- Have you ever discussed issues related to data privacy with your child? What advice do you give? Has your stance changed at all as your child has matured? (e.g. "don't post your full name, address, school schedule, etc. etc. online, don't agree to meet strangers")
- How do you discuss privacy and consent with your child when it comes to their social media use? For example, do you give them behavioral guidelines about when it is and is not appropriate to photograph or take video of others? Make suggestions about the content of their posts (such as discouraging gossip, or not talking about teachers vs. peers)?
- How do you handle a situation where your child is exposed to a digital device or service that you would not want them to use because of privacy concerns? For example, what would you do if you learned that your child was playing with a

"smart" toy that recorded their conversations while at a friend's house? What about if they were participating in a livestream broadcast, or interacting with strangers through a video game console?

- How do you handle situations where another person has shared information about your child that you/they wished to keep private? (e.g. an adult relative or friend sharing photos or videos of their child without asking; a peer broadcast their child or their child's personally identifying information online)
- Have you ever taught your child any specific privacy or safety measures aimed at protecting their data from police or other law enforcement agencies? If so, what advice have you given?
    - Have you and your child ever discussed your child's rights over the data on their mobile device while at school? For example, do they know that they are not required to delete or turn over content on their device if an administrator insists?
- Have you and your child ever discussed strategies they could use to protect themselves from harassment in digital spaces? What kinds of problems are you/your child most concerned by? How do you mitigate them?

REFERENCES

Aguilar, E. (2013). Update: Gov. Jerry Brown signs bill increasing online privacy for minors in California. 89.3 KPCC.

Anderson, M. (2015). Parents, teens and digital monitoring. *Pew Internet and American Life Project*, 1–26.

Andrewsi, L. (2012, February 4) Facebook is Using You. *The New York Times*.

Berkman Center for Internet & Society. (2002). Effect of the US Patriot Act on Internet Privacy.

Bernard, H. R. (2002). *Research methods in anthropology : qualitative and quantitative approaches*. (3rd ed.). Oxford, England: AltaMira Press.

boyd, danah. (2014). *It's complicated : the social lives of networked teens*. Yale University Press.

Brandeis, L., & Warren, S. (1890). The Right to Privacy. *Harvard Law Review*, *IV*(5).

C.A. Legis. S.B. 568. An act to add Chapter 22.1 (commencing with Section 22580) to Division 8 of the Business and Professions Code, relating to the Internet, 2013.

Caruso, D. (1998, April 13). An On-line Tug-of-War over Consumers' Personal Information. *The New York Times*, 5.

Chairman, R. P., Anthony, S. F., & Thompson, M. W. (2000). Federal Trade Commission.

Chazan, D. (2016). French parents "could be jailed" for posting children's photos online - Telegraph.

Christopher, A. (2014). Common Core State Standards and Technology Integration: a Study of Teachers' Experiences After Professional Development. (Doctoral dissertation, University of Memphis 2014). ProQuest Publishing

Cohen, J. E. (2012). Reimagining Privacy A Decentered Model of Subjectivity, 1–21.

Cohen, S. (1973). *Folk devils and moral panics : the creation of the Mods and Rockers*. Paladin.

Collins, K. (2017). Minnesota and Illinois have introduced legislation to protect internet users' private data — Quartz.

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology*, *13*(1), 3–21.

Discrimination by Type. (n.d.). In *US Equal Employment Opportunity Commission: Laws, Regulations & Guidance*. Retrieved April 12, 2017, from https://www.eeoc.gov/laws/types/

Facebook: 10 milestones on the way to social success. (2010, October 7). *The Telegraph*

Family Educational Rights and Privacy Act Regulations (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99, 2015.

Family Online Safety Institute. (2016). *Kids and the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots.*

Family Online Safety Institute. (2015). *Parents, Privacy & Technology Use*.

Family Online Safety Institute. (2014). *Parenting in the Digital Age.*

Family Online Safety Institute. (2012). *The Online Generation Gap: Executive Summary.*

Federal Trade Commission, 16 CFR Part 1. (2016). Adjustment of Civil Monetary Penalty Amounts.

Federal Trade Commission. (2013). *The Children's Online Privacy Protection Rule: a Six-Step Compliance Plan for Your Business.*

Federal Trade Commission. (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace.*

Federal Trade Commission. (1996). *FTC: Consumer Privacy Comments Concerning the Coalition for Advertising Supported Information and Entertainment-P954807*.

Fong, J. & Lee, D. [Vox] (2016, June 28). How Snapchat's filters work [video file]. *Vox Media*. Retrieved from https://www.youtube.com/watch?v=Pc2aJxnmzh0

Fung, Brian (2017, March 28). The House just voted to wipe away the FCC's landmark privacy protections. *The Washington Post*.

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Pub. Co.

Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others | US news | The Guardian.

Hayes, A. (2014). An Examination of the Common Core State Standards and Technology Standards Across the United States. (Doctoral dissertation, Tennessee State University, 2014). ProQuest Publishing.

Hild, K. (2016). Digital Literacy Education: are Existing Standards Providing Students with the Right Information?. Unpublished manuscript, Georgetown University.

Johnson, S. B., Blum, R. W., & Giedd, J. N. (2009). Adolescent maturity and the brain: the promise and pitfalls of neuroscience research in adolescent health policy. *The Journal of Adolescent Health : Official Publication of the Society for Adolescent Medicine*, *45*(3), 216–21.

Kessler, S. (2011, March 14). Children's Consumption of Digital Media On The Rise. *Mashable*.

Kunkel, D. "Children and Host-Selling Television Commercials." Communication Research 15 (1988): 71-92.

Kupfer, J. (2013). Privacy, Autonomy, and Self-Concept, *24*(1), 81–89.

Lewis, G. (2016). The Kid Behind the "Damn, Daniel" Meme Got Swatted Last Night - Vice.

Madden, M., Lenhart, A., & Cortesi, S. (2013). Teens, Social Media, and Privacy. *Pew Research Center and the Berkman Center for Internet & Society.*

Manches, B. A., Duncan, P., Plowman, L., & Sabeti, S. (2015). Three questions about the Internet of things and children, *59*(1).

Marcus, S. (2010, August 5). A Brief History of 9 Popular Blogging Platforms. *Mashable.*

Maslakovic, M. (2017). GPS trackers for kids: Best wearable devices to keep your children safe. getsandwearables.com/2017/02/19/best-wearable-devices-to-keep-your-children-safe/

Matyszczyk, C. (2015). Samsung changes Smart TV privacy policy in wake of spying fears - CNET.

McMeley, C., & Seiver, J. D. (2016). 1st Circuit and FTC Address Definitions of "PII," While Michigan Amends Privacy Law to Remove Statutory Damages - Advisories & Blogs - Davis Wright Tremaine.

Montgomery, K. C. (2007). *Generation Digital : politics, commerce, and childhood in the age of the internet*. MIT Press.

Morozov, E. (2012, November 27). In Soviet Russia, Book Reads You. *Slate*. Retrieved from http://www.slate.com/articles/technology/future_tense/2012/11/coursesmart_analytics_whispercast_the_danger_of_software_that_monitors_students.html

Newman, L. H. (2016). NY Cracks Down on Mattel and Hasbro For Tracking Kids Online | WIRED.

Ng, A. (2017). At New York Toy Fair, smart toys raise privacy questions - CNET.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 101–139.

Ofcom. (2016). Children and parents: media use and attitudes report. https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*, *57*(6), 1701–1777.

Porup, J. M. (2016). "Internet of Things" security is hilariously broken and getting worse.

Poulsen, K. (2006). MySpace Predator Caught by Code. *Wired*.

Reidenberg, J. R. (2000). The Data Surveillance State in the United States and Europe, (C 364).

Rich, J. (2016). Keeping Up with the Online Advertising Industry. *Federal Trade Commission*.

Smith, M. S., Seifert, J. W., McLoughlin, G. J., & Moteff, J. D. (2002). The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government.

Solomon, W. S., & McChesney, R. W. (1993). *Ruthless criticism : new perspectives in U.S. communication history*. University of Minnesota Press.

Solove, D. (2017). The U.S. Congress Is Not the Leader in Privacy or Data Security Law - TeachPrivacy.

Solove, D. J. (2007). *The Future Of Reputation: Gossip, Rumor, And Privacy On The Internet.* Yale University Press.

Solove, D. J. (2006). A Brief History of Information Privacy Law. In K. J. Mathews (Ed.), *Proskauer on privacy : a guide to privacy and data security law in the information age* (pp. 1–46).

Solove, D. J., Washington, G., & Richards, N. M. (2007). Privacy's Other Path : Recovering the Law of Confidentiality Privacy's Other Path : Recovering the Law of, *123*.

Springhall, J. (1998). *Youth, popular culture and moral panics : penny gaffs to gangsta-rap, 1830-1996*. Macmillan.

Stanford History Education Group. (2016). Evaluating information: The cornerstone of civic online reasoning, 29.

State Laws Related to Internet Privacy. (2017, January 5). National Conference of State Legislatures. http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Stenovec, T. (2011). Myspace History: A Timeline Of The Social Network's Biggest Moments | The Huffington Post.

U.K. Information Commissioner's Office. (2015). Questions Raised Over Children's Websites and Apps.

United States v. Jones. Supreme Court of the United States. 2012.

Ward, V. (2015, July 28). Children Should Be Able to Delete Photos from the Web. *The Telegraph*.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *Faculty Scholarship Series*. New Haven, CT: Yale Law Journal (113), 1151-1221.

Wilcox, B. L., Kunkel, D., Cantor, J., Dowrick, P., Linn, S., & Palmer, E. (2004). Report of the APA Task Force on Advertising and Children. Retrieved from http://www.apa.org/pi/families/resources/advertising-children.pdf

Williams, P. (2006). MySpace, Facebook attract online predators. *NBC Nightly News with Brian Williams*.

Yershov v. Gannett Satellite Information Network, Inc. (1st Cir. 2016)

Zittrain, J., & Sauter, M. (2010). Everything You Need to Know About Wikileaks - MIT Technology Review.

Zwitter, A. (2014). Big Data ethics. *Big Data & Society*, *1*(2), 1-6.