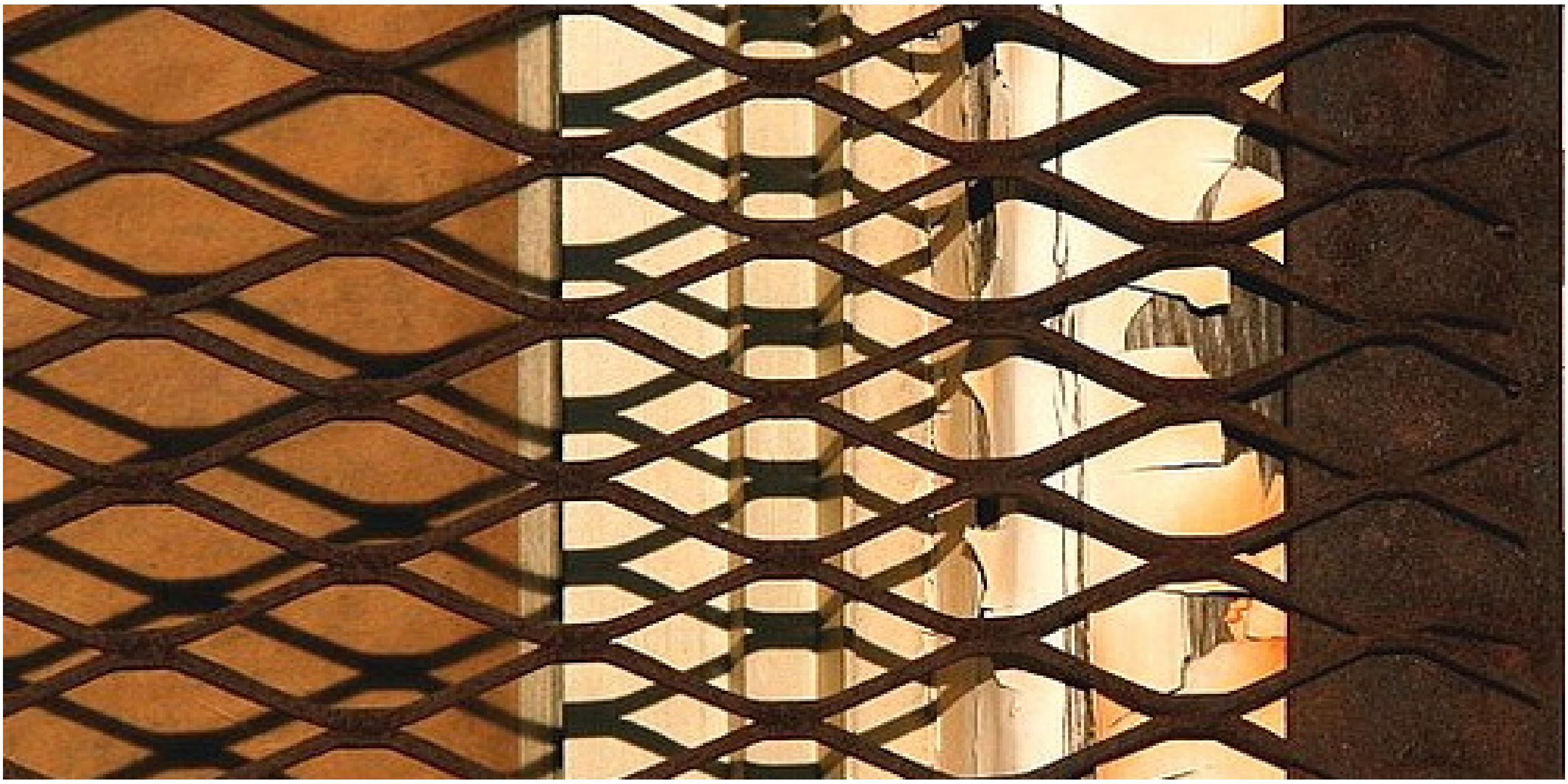
Berkman
The Berkman Center for Internet & Society
at Harvard University

Youth, Privacy and Reputation

Literature Review



Alice E. Marwick, Berkman Center and New York University

Diego Murgia Diaz, Berkman Center and Harvard Law School

John Palfrey, Berkman Center and Harvard Law School

March 29, 2010

The Berkman Center for Internet & Society at Harvard University
23 Everett Street • Second Floor • Cambridge, Massachusetts 02138
+1 617.495.7547 • +1 617.495.7641 (fax) • cyber@law.harvard.edu
http://cyber.law.harvard.edu

Cover photo:
Many Layers by Evelyn Berg (ebergcanada) on FLICKR
http://www.flickr.com/photos/eberg/3204692747/

Table of Contents

1. Introduction

Many adults worry about children and teenagers' online privacy, predominantly due to a perception that youth put themselves at risk for harassment and solicitation by revealing personal information, usually to marketers or on social networking sites (Aidman 2000; Giffen 2008; Read 2006). First, commercial websites and advertising networks are said to manipulate children into providing personal data which is bought, sold, and used for monetary gain (Cai & Gantz 2000; Montgomery & Pasnik 1996; Moscardelli & Liston-Heyes 2004; Youn 2009). Second, recent privacy worries are centered around secrecy, access, and the risks that "public living" on sites like Facebook, MySpace, and YouTube poses from educational institutions, future employers, pedophiles, and child pornographers (Palfrey et al. 2008; Lenhart & Madden 2007; Youn 2009). These concerns can translate to blaming youth for their carelessness, with the frequently-cited maxim that "youth don't care about privacy" (Kornblum 2007; Nussbaum 2007; Moscardelli & Liston-Heyes 2004). At the same time that youth are castigated for their openness, children and teenagers are under increasing surveillance at home and school, facilitated by Internet filters, mobile phones, and other monitoring technologies (Berson & Berson, 2006; Hope, 2005).

Often, young people are viewed on one side of a generational divide (Herring 2008). "Millennials" or "digital natives" are portrayed as more comfortable with digital technologies and as having significantly different behaviors than their "digital immigrant" parents (Palfrey & Gasser 2008; Solove 2008; N. Howe & Strauss 2000). There is a risk of this discourse exoticizing the experience of young people from an adult perspective, given the fact that adults perform most of the research on young people, create the technologies that young people use, and produce media commentary on children and teenagers (Herring 2008). Much of the popular media's commentary on young people lumps children and teenagers together using a "generational" rhetoric that flattens the diverse experiences of young people in different contexts, countries, class positions and traditions.

For many of today's young people, peer socialization, flirting, gossiping, relationship-building, and "hanging out" takes place online (boyd 2008; Ito et al. 2008; Herring 2008). Young people primarily use online technologies to talk with people they already know. Sharing information through social network sites or instant messenger reinforces bonds of trust within peer groups.

The idea of two distinct spheres, of the "public" and the "private," is in many ways an outdated concept to today's young people. Much of the studies of privacy online focus on risk, rather than understanding the necessity of private spaces for young people where they can socialize away from the watching eyes of parents or teachers. These seeming contradictions demonstrate how understandings of risk, public space, private information, and the role of the Internet in day-to-day life differ between children, teenagers, parents, teachers, journalists, and scholars.

The scope of this literature review is to map out what is currently understood about the intersections of youth, reputation, and privacy online, focusing on youth attitudes and practices. We summarize both key empirical studies from quantitative and qualitative perspectives and the legal issues involved in regulating privacy and reputation. This project includes studies of children, teenagers, and younger college students. For the purposes of this document, we use "teenagers" or "adolescents" to refer to young people ages 13-19; children are considered to be 0-12 years old. However, due to a lack of large-scale empirical research on this topic, and the prevalence of empirical studies on college students, we selectively included studies that discussed age or included age as a variable. Due to language issues, the majority of this literature covers the United States, the United Kingdom, the European Union, and Canada.

2. Privacy

2.1 Concepts of Privacy

In any meaningful discussion of privacy, it is essential to clarify what the term privacy means. First, we must distinguish between the concept of privacy and the right to privacy (Solove & Schwartz 2009). The former involves what privacy entails and how it is to be valued, while the latter refers to the extent to which privacy is and should be legally protected. In constructing a concept of privacy, we should look beyond the law because what the law *does* protect is not necessarily what it necessarily *should* protect (Solove & Schwartz 2009).

The concept of privacy has presented various difficulties for privacy scholars in defining what is perceived to be an ambiguous term (Solove & Schwartz 2009; Wong 2005). Definitions have ranged from the famous conception of the "right to be let alone" (Warren & Brandeis 1890), to the right to control information of oneself (Westin 1967). In their influential article, "The Right to Privacy", Warren and Brandeis articulated the argument for the importance of individual privacy and described it as one's "right to be let alone" (1890, p.193). Warren and Brandeis noted that the technological advances in photography in the latter part of the nineteenth century rendered past privacy doctrines inadequate (Warren & Brandeis 1890, p.211). Thus, they argued that broader legal principles needed to be developed to keep pace with new technology (Warren & Brandeis 1890).

Westin provides a two-fold definition of privacy, holding that it is a:

> [C]laim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy, or, when among larger groups, in a condition of anonymity or reserve (1967).

If privacy is viewed as a control device, the unauthorized disclosures of personal information subjects individuals to the involuntary scrutiny of others (Martin 1998). Martin notes that individuals may suffer from the presumptions that others develop from this unauthorized scrutiny. Therefore, a fear of inaccuracy resulting from unauthorized information analysis restricts people's freedom to act in the way they wish (1998, p.818).

Solove argues that the many conceptions of privacy can be divided into six general headings: (1) the right to be let alone; (2) limited access to the self, or the ability to shield oneself from unwanted access by others; (3) secrecy, or the concealment of certain matters from others; (4)

control over personal information, or the ability to exercise control over information about oneself; (5) personhood, or the protection of one's personality, individuality, and dignity; and (6) intimacy, which is to say, control over, or limited access to, one's intimate relationships or aspects of life (2002).

2.2 Need for Balance

Some scholars have argued that privacy is a necessary requirement for life in modern democratic states (Warren & Brandeis 1890; Westin 1967), and that it contributes to an individual's personal autonomy and dignity. However, privacy is not an absolute right under law; an individual's right to privacy may be outweighed by other interests, such as national security and the rights and freedoms of others (European Convention on Human Rights 1950). Consequently, trade-offs must be made to promote a balance between these seemingly competing interests (Westin 1967; Nemati et al. 2003). The need for balance has led to longstanding discussions about how to assess the value of these interests and accordingly, how to determine what is a reasonable trade-off (Cullen & Reilly 2007). Regardless of the philosophy one adheres to promote such a balance, Westin notes that "either too much or too little privacy can create imbalances which seriously jeopardize the individual's well-being" (1967, p.40).

2.3 Privacy and Technology

Digital privacy has been a consistent concern since the Internet became a popular medium in the 1990s. Helen Nissenbaum divides the concerns over new technologies into three categories: (1) monitoring and tracking, (2) dissemination and publication, and (3) aggregation and analysis (2009). The first category involves concerns about the widespread monitoring facilitated by surveillance technologies such as closed-circuit television systems (CCTV), RFID tags, electronic toll collection, facial recognition systems, tracking cookies, and behavioral targeting and marketing (Andrejevic 2007; Monahan 2006; Turow 2006). These technologies are used by both governments and private entities to observe and track the behavior of individuals and larger populations both on and offline, and scholars have expressed a variety of concerns about their impacts on individual liberty and privacy law.

Second, the proliferation of computers, communication networks, and digital information has created an environment in which personal details are more readily available than ever before (Cullen & Reilly 2007; Palfrey & Gasser 2008). It is common for people that live their lives mediated by digital technologies to disclose, knowingly or unknowingly, personal information online. Once digitized, such information is virtually irretrievable and may be intercepted or purchased by commercial entities, governments, or individuals for marketing or other more sinister purposes (Ciocchetti 2007; Palfrey & Gasser 2008; Solove 2008). Moreover, this information can be spread and transmitted further and wider than ever before; for example, the publication of court records online or scanning old photographs and publishing them to Facebook (Nissenbaum 2009).

Third, aggregation and analysis involving large databases are increasing the possibility that individual privacy may be invaded in new and more substantial ways. Commercial data brokers, like ChoicePoint, are in the business of piecing together people's personal data to form an individual profile or "digital dossier" (Solove 2004). In order to better appreciate the privacy problems created by databases, Solove draws upon the depiction of a shadowy and unconstrained bureaucracy in Franz Kafka's novel "The Trial". Solove argues that the increasing use and dissemination of personal information creates a "Kafkaesque world of bureaucracy, where we are increasingly powerless and vulnerable, where personal information is not only outside our control but also subjected to a bureaucratic process that is itself not adequately controlled. This generalized harm already exists; we need not wait for specific abuses to occur" (2004, p.96).

The more comprehensive the data aggregation, the more attention such aggregation deserves because of potential privacy risks (Ciocchetti 2007). Although data brokers have the ability to gather personal information without the Fourth Amendment restrictions placed on the government, they work closely and share information with the government and with virtually anyone who pays for it, including medical, financial and insurance industries (Mills 2008). Problematically, the information in these digital dossiers might be used to discriminate against individuals. Imagine "if health-insurance premiums were calculated based on data from online food orders, or if an online merchant's pricing system discriminated among customers based on their income or spending patterns" (Palfrey & Gasser 2008, p.59). Digital dossiers present other problems: unauthorized access to this cache of personal information may result in cases of identity theft, stalking, harassment, and other invasions of privacy (Ciocchetti 2007; Palfrey & Gasser 2008; Solove 2008).

2.4 Third-Party Data Problem

The Fourth Amendment to the United States Constitution requires that searches by the government must be reasonable (U.S. Const. amend. IV). According to the Supreme Court, an individual has an expectation of privacy where (1) the individual possesses a subjective expectation of privacy; and (2) that expectation is "one that society is prepared to recognize as "reasonable"" (*Katz v. United States,* 389 U.S. 361 (1967)). However, information "knowingly exposed to the public" is not entitled to Fourth Amendment protection, (*Katz,* 389 U.S. at 351) establishing what Daniel Solove refers to as the "secrecy paradigm": Where information is voluntarily shared with another party, it may be legally obtained without a warrant (Solove 2004). Accordingly, citizens have no reasonable expectation of privacy in data they give to third parties (*United States v. Miller,* 425 U.S. 435, 442-43 (1976)). This standard applies equally to information truly open to the public as well as information voluntarily shared with a third party within the context of a confidential relationship, such as a business (*Miller*, 425 U.S. at 443).

Third-party doctrine governs the Fourth Amendment privacy protection for information revealed to third parties (Solove 2005). Essentially, when a person reveals private information to a third party, that individual “assumes the risk” that the third party may reveal the information to authorities (*United States v. Jacobsen*, 466 U.S. 109, 117 (1984)). If the third party willingly reveals that information to the authorities, the government does not violate the Fourth Amendment by using it. Scholars argue that the third party doctrine poses a substantial threat to privacy nowadays in light of the dramatic extent to which third parties hold personal information.

> The increasing amount of personal information flowing to the government poses significant problems with far-reaching social effects. Inadequately constrained government information-gathering can lead to at least three types of harms. First, it can result in the slow creep toward a totalitarian state. Second, it can chill democratic activities and interfere with individual self-determination. Third, it can lead to the danger of harms arising in bureaucratic settings. Individuals, especially in times of crisis, are vulnerable to abuse from government misuse of personal information. Once government entities have collected personal information, there are few regulations of how it can be used and how long it can be kept. The bureaucratic nature of modern law enforcement institutions can enable sweeping searches, the misuse of personal data, improper exercises of discretion, unjustified interrogation and arrests, roundups of disfavored individuals, and discriminatory profiling (Solove 2002).

Professor Palfrey argues that the “third-party doctrine becomes increasingly problematic as technology, and usage of it, evolves” (2008, p. 288). One of the primary concerns that arise out of this fast-changing state of affairs regards the convergence of the public and the private. The concern is “whether citizens are able to make reasonable choices about how they lead lives mediated by these technologies and what the consequences of those choices might be with respect to what the state can come to know about them” (Palfrey 2008, p. 281).

“What matters from the citizen's perspective is whether he or she has a reasonable expectation that the activities under surveillance are taking place in public or private” (Palfrey 2008, p. 283). According to Professor Palfrey, this perspective has three important problems in the digital age. First, “the activity might be taking place in a context that the citizen believes is "private," but where a third party is recording that activity” (Palfrey 2008, p. 283-4). For example, since young people constantly perceive their online audiences as more (and occasionally less) "private" than they really are, they might disclose information to a page that they maintain on a social network site to which only friends have access. Although the information might be shared in a context which feels "private", it is plainly open to surveillance of multiple kinds, without Fourth Amendment protection (Palfrey 2008, p. 284).

The second problem is that nowadays it is difficult for citizens to keep anything truly private from third parties because an average citizen's life "is increasingly mediated by digital technologies, her social life, her work life, her civic life, and any other lives she leads are often led partly in digital public spaces" (Palfrey 2008, p. 285). Finally, it is extremely difficult for the average citizen to keep up with the pace of technological change (Palfrey 2008, p. 285). As Palfrey notes, digital technologies are developing at a very fast pace, "such that even technology experts have little sense of what is even commercially available in fields tangentially related to their own. Few people would be knowledgeable enough about digital technologies to have an effective sense of what information they are sharing is publicly accessible and what is private" (Palfrey 2008, p. 285).

2.5 Youth, Privacy, and Technology

Much of the literature about youth and online privacy falls into one of two categories, both of which focus primarily on risk. The first expresses concern about commercial websites and advertising networks that manipulate children into providing personal data which is bought, sold, and used for monetary gain, falling into Solove's categories of "unwanted access by others" and "control over personal information", generally referred to as "consumer privacy" (Cai & Gantz 2000; Montgomery & Pasnik 1996; Moscardelli & Liston-Heyes 2004; Youn 2009). For example, the Federal Trade Commission (FTC) has stated that the collection of personal information from young children presents "unique privacy and safety concerns because of the particular vulnerability of children, the immediacy and ease with which information can be collected from them, and the ability of the online medium to circumvent the traditional gatekeeping role of the parent" (Federal Trade Commission 1998, pp.4-5). Early studies of children online found that they were unable to distinguish advertising content from non-commercial content, such as banner advertising (Henke 1999). This concern inspired the Children's Online Privacy Protection Act (COPPA) in 1998, which requires parental permission to collect information from children under 13 (Youn 2005). However, in follow-up studies, children displayed savvy about online advertising, and the earlier findings were explained by the novelty of the Internet at the time (Henke 2002).

Since then, the positioning of youth as innocent victims of online scams has been partially replaced with a view of children and teenagers as "digital natives," some of whom are increasingly savvy about new technologies and critical about marketing and media practices (Palfrey & Gasser 2008; Howe & Strauss 2000). More recent privacy concerns are thus less focused on consumer privacy and more centered around secrecy, access, and the future risks that "public living" on sites like Facebook, MySpace, and YouTube poses from educational institutions, future employers, pedophiles, and child pornographers (Lenhart & Madden 2007; Youn 2009; Schrock & boyd 2008). Although "privacy might be a problem for anyone who leads a life mediated in part by digital technologies", the problem is said to be more acute for young people "because we are just at the beginning of the digital age" (Palfrey & Gasser 2008, pp.61-

62). Scholars claim that young people will be the first to experience the aggregated effect of living a digital mediated life, with the corresponding creation of various identities and digital dossiers over a long period of time. Solove describes modern “architectural problems” related to privacy, which involve “the creation of the risk that a person might be harmed in the future” (Solove 2005, p.487). Unfortunately, these risks are often vague and currently there are no empirical studies on the reality of these risks, despite this emphasis (Schrock & boyd 2008).

We discuss both these bodies of literature in some detail, but it is important to note that there are alternate conceptualizations of privacy that remain understudied with regard to youth. For instance, although this literature review focuses on privacy and technology, we were interested in perspectives on children and privacy in the day-to-day “offline” world as well. However, we found few recent studies about children, teens, and privacy with regards to other aspects of life, such as their experiences at home, at school, and in public; privacy seems to be inextricably intertwined with “online privacy.” For example, there is little work about the impact of surveillance and monitoring on youth, or how this affects their understanding of privacy. Despite this, offline privacy is important to young people, who consistently express concerns about parents and teachers viewing personal information and refer disparagingly to adults “snooping” (Livingstone 2006; Ito et al. 2008; Grant 2006; Herring 2008).

In Sonia Livingstone’s ethnographic studies of children using the Internet at home, she points out that most research on children and privacy focuses on external threats to privacy, rather than children’s own conceptions of privacy. She writes, “Children seek privacy, but as a means to an end, not an end in itself”:

> ...they may use the opportunity of private spaces online to indulge in silly, rude or naughty behavior, to experiment with new identities, to seek confidential advice on personal matters; to eavesdrop on the interactions of others, to meet people from far-off places or from the next street, and, most of all, to engage in uninterrupted, unobserved immersion in peer communication (2006, p.132)

For such youth, privacy is about being in control of their own actions, information, and choices, including the ability to share personal information online and participate in online socializing. This includes privacy *from* adults, especially parents and teachers. Ian Grant emphasizes the importance of understanding online privacy in “the contextual, everyday lives of young people” rather than on an abstract level (2006, p.4). Since social media is an enormously significant part of youth culture—games, social network sites, video-sharing sites, gadgets, and mobile phones all contribute significantly to peer connections and youth socialization in general—without a clear understanding of how these technologies are used by young people, analyses of privacy will be incomplete (Ito et al. 2008).

3. Attitudes towards Privacy

There is widespread consensus that children and teenagers show less concern than adults about privacy (Moscardelli & Liston-Heyes 2004, p.51; Edwards & Brown 2009; Palfrey & Gasser 2008). Surprisingly, there are few empirical studies that show this conclusively, particularly when compared to adults. For example, an early study by Turow and Nir found that while 79% of young people (10-17 year olds) displayed concern about privacy, they were more willing than adults to provide personal information in exchange for a free gift (Turow & Nir 2000). Moscardelli and Liston-Heyes compared their survey of 713 13-19 year olds with an e-mail survey of adult consumers (Sheehan & Hoy 2000) and found that adolescents scored considerably lower than adults in terms of privacy concerns. However, they point out that the survey methods between the two studies are different and that the lack of previous empirical research on adolescents and privacy makes it difficult to compare data (2004).

Studies demonstrate that it is a mistake to group all youth together. Not only do privacy attitudes differ by age (Lenhart & Madden 2007; Lwin et al. 2008; Steeves & Webster 2008), but also within similar age cohorts. Grant's study of 200 Scottish teenagers identified three categories of attitudes towards privacy. *Naïve dabblers*, who didn't know very much about online privacy, were likely to be infrequent Internet users. *Open-minded liberals* were relatively more aware of online privacy, but assumed it was not a serious concern and that revealing personal information would have minimal negative consequences. *Cynical concealers* were the most concerned about issues of privacy and the most likely to engage in evasion or manipulation; these teens tended to be the older and more experienced Internet users (2006, pp.7-9). These user categories map fairly accurately to those of adults identified in a series of studies by Dr. Alan Westin: *privacy fundamentalists*, who are extremely concerned; *privacy unconcerned*, who do not know much about privacy and dismiss consequences; and *privacy pragmatists*, who are concerned about privacy but still provide personal information online (Kumaraguru & Cranor 2005; Westin 2003). This variety among both youth and adults suggests that it is difficult to predict attitude based on age cohort.

Moscardelli and Liston-Heyes suggest that differences between adults and young people with regard to privacy may be due to lack of knowledge about privacy. Their study concluded that teens whose parents monitor Internet use or browse the Internet with them show higher rates of privacy concerns than those whose parents do not (Moscardelli & Divine 2007, p.243; Moscardelli & Liston-Heyes 2004, p.53).

However, this may also be due to the differences in social context between children, teenagers, and adults, and how behavior that *adults* promote as privacy-protective is not necessarily congruent with children's social behavior and social roles (Steeves & Webster 2008, p.14). Studies that investigate youth concepts of privacy do show demonstrated concern. A large, multi-methodological study of more than 7,000 college students at 29 American universities revealed that three-quarters were concerned with privacy, such as the security of passwords, social security numbers, and credit card numbers. They were not, however, concerned about sharing personal information on sites like Facebook; social networking sites were viewed as relatively "private" spaces, and the consequences were deemed insignificant (Jones et al. 2009). Likewise, a study of 326 high school students concluded that teenagers take a "risk-benefit" approach to sharing personal information online: "a higher level of risk perception of information disclosure led to less willingness to provide information… as teenagers perceived more benefits from information disclosure, they were more willing to provide information" (Youn 2005). A follow-up study of younger children (12 year-old seventh graders) concurred (Youn 2009).

Most young people socialize online with people they know personally (boyd 2007; Ito et al. 2008; Palfrey & Gasser 2008) Revealing "information on a website and writing blog posts and comments feels more akin to chatting with friends, writing a diary, or talking on the telephone than like broadcasting live on television, publishing a novel, or addressing a crowded auditorium" (Solove 2007, p.198). Indeed, studies show that young people conceptualize the Internet as a *private* space where they can share secrets and talk to their friends (Livingstone 2005; Steeves & Webster 2008; Ito et al. 2008), behavior that intrinsically requires the sharing of personal information. For example, sharing email addresses and passwords with friends (demonstrated in 31% of sampled students) was not seen as risky (Steeves & Webster 2008, p.10). Instead, young people viewed this as an easy way for their friends to check email or social networking sites for them, or as a mechanism to demonstrate trust (similar to knowing a locker combination). Thus, provision of personal information, which is often necessary to maintain intimacies with real-life friends, must be seen within a social context such as a peer group, rather than the public at large (Livingstone 2008, p.400). Using Youn's protection motivation framework, the perceived social benefits of online information-sharing outweighed any potential risks (Christofides et al. 2009).

Moreover, for youth, "privacy" is not a singular variable. Different types of information are seen as more or less private; choosing what to conceal or reveal is an intense and ongoing process (Livingstone 2008, p.404). Rather than viewing a distinct division between "private" and "public," young people view social contexts as multiple and overlapping. For instance, college students are far more concerned with parents or employers viewing social network profiles than they are friends or peer group members (Christofides et al. 2009). Indeed, the very distinction between "public" and "private" is problematic for many young people, who tend to view privacy in more nuanced ways, conceptualizing Internet spaces as "semi-public" or making distinctions between different groups of "friends" (West et al. 2009). In many studies of young people and privacy, "privacy" is undefined or is taken to be an automatic good. However, disclosing information is not *necessarily* risky or problematic; it has many social benefits that typically go unmentioned. For a comprehensive look at the literature on online youth and risk, see Schrock and boyd, 2008.

4. Youth Experiences of Privacy

4.1 Privacy in the Home

Traditionally, the home has been seen as a "private" space and the "family" as a privately regulated sphere (Turow 2001). However, viewing "private" and "public" as a dichotomy has a long and contentious history and researchers and philosophers from feminist theory, economics, political theory, and so forth have explored and debated this concept in depth, which is beyond the scope of this paper (West et al. 2009). The extent to which children view their home as a private realm is variable, since children are often closely watched and monitored in their own home. The "home" is further fragmented into sections; living and family rooms are more 'public', while children's bedrooms are conceptualized as individual, private space (Bovill & Livingstone 2001). Regardless, the home is a primary space for accessing technologies and media, as well as negotiating the boundaries of private and public space with parents, a frequent source of conflict (Van Rompaey et al. 2002; McLean & Griffiths 2009; West et al. 2009). While the Internet, television and other media are viewed by some as an intrusion of the public sphere into the private (McLean & Griffiths 2009), as children are systematically excluded from public places through the elimination of local teen centers, regulation of malls, and so forth, the media-rich bedroom is framed as a safe alternative to going out in public (Livingstone 2005, p.43; boyd 2008).

Not all families are equal in terms of media use. Several studies categorized three types of families: *media-poor* (low media density, including TV, telephone, and audio), *intermediate* (average media density, such as more than one TV and audio media), and *multimedia* (high media density, including Internet, e-mail, and so forth) (Van Rompaey et al. 2002; Livingstone 2007). Homes that own Internet-enabled computers may place them in a common area or in a child's bedroom or similarly private space. The extent to which the computer is public affects the way it is used; like other media like television and music, having access to a computer and Internet in the bedroom increases the use of this media (Livingstone 2007).

Many children in ethnographic studies see Internet monitoring and keylogging at home as snooping and a violation of their privacy, much like searching their school bag, reading their diary, or listening in on a phone call (Livingstone 2006; Devitt & Roker 2009). Parents who attempted to check their children's online journals or social network sites were seen as controlling, invasive, and "clueless" (Ito et al. 2008, p.19). In West et. al's study of parents on Facebook, researchers found that young people adhered to "a notion of public that excludes the family" (2009, p.621). Teenagers did not want their parents to view their social network site profiles, pictures, or status updates, and saw parents joining Facebook as intrusive and embarrassing (West et al. 2009).

4.2 Privacy in Schools

There are several problematic issues with regards to children's privacy in schools. First, in the United States, the *No Child Left Behind Act* requires K-12 schools to store information about students electronically, which can include "pregnancy, mental health information, criminal history, birth order, victims of peer violence, parental education, medical test results, and birth weight" (Calabrese 2009). However, the aggregation of this information into electronic databases and the lack of weak data protections put young people at risk for the dissemination of highly personal data. A comprehensive review by the Center for Law and Information Policy at Fordham Law School concluded:

> We reviewed publicly available information from all 50 states and found that privacy protections for the longitudinal databases were lacking in the majority of states. We found that most states collected information in excess of what is needed for the reporting requirements of the No Child Left Behind Act and what appeared needed to evaluate overall school progress. The majority of longitudinal databases that we examined held detailed information about each child in what appeared to be non-anonymous student records. Typically, the information collected included directory, demographic, disciplinary, academic, health, and family information. Some striking examples are that at least 32% of the states warehouse children's social security numbers, at least 22% of the states record children's pregnancies, at least 46% of the states track mental health, illness, and jail sentences as part of the children's educational records, and almost all states with known programs collect family wealth indicators. We found that, given the detailed and sensitive nature of the information collected, the databases generally had weak privacy protections (Reidenberg & Debelak 2009).

Second, in the United States, two federal acts—*The Neighborhood Children's Internet Protection Act* (NCIPA) and *The Children's Internet Protection Act* (CIPA) mandate the use of Internet filters by schools and libraries receiving federal funds (Yan 2005). These filters have been criticized for blocking valuable information and disproportionately affecting the Internet access of children who do not have access to the Internet at home (Gottschalk 2006; Heins et al. 2006). Many schools also monitor and track children's Internet use or do not allow children to use the Internet unsupervised. Andrew Hope's three studies of Internet access in UK schools found that a variety of physical and virtual surveillance techniques were used to prevent students from accessing pornography, social media, chat rooms, and video games, including watching children use the computer and tracking and storing visited sites (Hope 2005; Hope 2007; Hope 2009).

Finally, throughout the United States, schools have adopted advanced security measures in response to highly-publicized school shootings, such as metal detectors, x-rays inspection of student possessions, identification cards, locker searches, strip searches, security cameras, and so forth (Addington 2009). Although these measures clearly reduce student privacy, there is no conclusive evidence that they have positive effects on student safety (Addington 2009; Birkland & Lawrence 2009). Addington concludes that "students' rights are in a precarious position with increases in suspicionless searches and monitoring. In addition to the growing use of measures to monitor students, new technologies, such as Webcams and RFID tracking capabilities, appear to increase the level of intrusion" (2009, p.1441).

4.3 Surveillance

In many parts of the United States and Europe, young people are monitored while at home, at school, and in semi-public places like malls and parks, to the point where the "increased protection of children by monitoring them" is seen as "a central characteristic of modern childhood" (Fotel & Thomsen 2004, p.536). In their 2000 book *Millennials Rising,* Neil Howe and William Strauss claim this is the most "watched over generation in memory" (2000, p.9). Surveillance, or the monitoring of behavior and activities, is facilitated by technologies such as Internet tracking software, closed-circuit television (CCTV), mobile phones, baby monitors, GPS devices, and the like (Fotel & Thomsen 2004; Hope 2005; Nelson 2008).

Surveillance of young people can be divided into two broad categories: direct and remote. Direct surveillance requires actively watching a child, whether by driving them to an appointment or watching them use the Internet in a library. Remote surveillance is usually done via technology, typically filters or mobile phones (Fotel & Thomsen 2004; Pain et al. 2005). In both of these types of surveillance, the limits of mobility and access are determined in a negotiation between children and parents (Fotel & Thomsen 2004; Backett-Milburn & Harden 2004; Elsley 2004).

This surveillance has led to concerns about limiting children's mobility (Williams et al. 2005), the isolation and suspicion of young people (Giroux 2003), and increasing parental anxiety (Nelson 2008). Although there is little evidence about the extent of this surveillance or how many parents or schools engage in these practices, the perception of widespread monitoring has become so common that "the state in the UK can now openly question whether (urban) parents are good parents if they don't know where their children are at all times and have control over them" (Williams et al. 2005, p.2). Indeed, the surveillance of children is primarily linked to safety—e.g. knowing where a child is at all times prevents kidnapping, or observing children web surfing avoids encounters with upsetting content. Thus, surveillance is framed in a language of protection and *care* (Lyon 2001, p.3) and children as intrinsically at risk (Nelson 2008, p.525). (For a comprehensive look at the literature on online youth and risk, see Schrock and boyd, 2008.)

At the same time, teenagers are often perceived as threatening, which results in restrictions on their movement through stores, public parks, and so forth. This dual view—that young people need protection in public space, and that young people are a threat to others in public space—has a long history (Valentine 2004). Both these discourses justify widespread monitoring. For example, Andrew Hope identifies three primary uses of security cameras in schools: "access control, conduct control, and evidence gathering" (2009, p.894). His survey of 8 English schools found that CCTV was used for all three, to monitor "dangerous outsiders" and crimes like petty theft and graffiti; to regulate student behavior, such as loitering in halls; and to provide evidence for disciplinary action. He argues that security cameras do not necessarily encourage self-policing among students; rather, they encourage youth engaged in punishable activities to limit them to unmonitored areas.

5. Influences on Privacy Attitudes and Practices

5.1 Parents and Family

Studies show that parental activity, such as discussions about privacy, monitoring Internet use, and browsing the Internet with their children, correlates positively with privacy concern, resulting in increased privacy-protective behavior such as decreased likelihood of disclosing personal information (Moscardelli & Divine 2007; Moscardelli & Liston-Heyes 2004; Steeves & Webster 2008; Youn 2008; Wirth et al. 2007). However, parental mediation, or activities carried out by parents to influence children's online behavior, can also be viewed as limiting the privacy of children and teens online. Although studies generally see parental mediation as a positive influence on children in terms of increasing media literacy, providing less personal information to websites, and so forth (Livingstone 2007), several ethnographic studies have found that children see mediation, Internet filtering, monitoring, and keylogging as privacy violations (Livingstone 2006; Grant 2006).

Parental mediation can be divided into three categories: *factual mediation,* which primarily involves educating children about media creation and business; *regulated* or *restricted mediation*, where parents make rules prohibiting or limiting certain actions; and *active* or *evaluative mediation,* where parents discuss media content with their children during or after experiencing it (Lwin et al. 2008; Eastin et al. 2006). Similarly, psychologists have divided overall parenting styles into four categories: *authoritarian* (high control and low warmth), *authoritative* (high control and high warmth), *indulgent* or *permissive* (low control and high warmth) or *neglectful* (low control and low warmth) (Rosen et al. 2008). A study of more than 500 American parents found that authoritative parents are most likely to use evaluative and restrictive mediation, particularly technological mediation (Eastin et al. 2006), resulting in the lowest rates of information disclosure and other "risky" behaviors like meeting online friends face-to-face among their children (Rosen et al. 2008). Generally, active mediation, like co-surfing, has more of an effect on privacy attitudes than regulated mediation such as filters (Youn 2008, p.381). A survey of 300 10-12 year olds and 350 13-17 year olds found that active mediation was more effective than regulated mediation in reducing the amount of personal information provided to commercial websites; children and teens whose parents actively mediated their Internet use had the lowest information disclosure of any group (2008, p.213).

Parents report high rates of both Internet filtering and monitoring. In a large survey of the parents of more than 900 American teens, 86% of parents claimed they regulated Web use, with 66% reporting time limits and 56% filtering software (Mesch 2009). The Pew Internet project found that 50% of teens' home computers had filtering software installed, and 35% of teens believed monitoring software was installed (Lenhart & Madden 2007, p.v). In a study of 749 dyads of American parents and teenagers found that 61% of parents claimed to restrict Internet use, and 44% had installed monitoring software (Wang et al. 2005, p.1253). However, the extent of parental monitoring is undetermined as studies are contradictory and teens report far lower filtering and supervision. Rosen et. al found that 60% of 500 American parents surveyed had no limits on Internet use and even those who claimed they knew what information their children were providing online underestimated that information provision (2008). Although in Wang's study a high percentage of parents claimed to mediate Internet access, only 38% of the teens in the sample said their parents had rules about using the Internet; in 40% of families, there were discrepancies between parents and children about the existence of Internet-related rules (Wang et al. 2005). Livingstone identifies similar disconnects between parental mediation reported by children and parents; she says "either parents overclaim, being less effective than they would hope, or that children underclaim, being less independent than they would hope" (2007, p.14). This is consistent with studies of parental restrictions on other types of media, such as television (Bovill & Livingstone 2001).

Indeed, critics say that leaving the responsibility for content regulation in the hands of parents is ineffective as most parents are inattentive or know less about the Internet than their technically-proficient children. Active Internet mediation is more difficult, as surfing the Internet tends to be a solitary activity, while watching television or movies is often done in a family co-viewing context (Littman 2000; Moscardelli & Liston-Heyes 2004).

5.2 Gender

Generally, girls are more likely to be concerned with privacy than boys, consistent with studies that show that women are more concerned with privacy than men (Lenhart & Madden 2007, p.iii; Moscardelli & Divine 2007, p.243; Moscardelli & Liston-Heyes 2004, p.53; Fogel & Nehmad 2009). Youn and Hall found that girls felt more vulnerable to privacy risks than boys. Girls identified these risks as feeling uncomfortable, the creation of potential conflicts with parents and teachers, receiving unsolicited e-mail and misuse of personal information. This perception resulted in girls curtailing their online activities more than boys, who were more likely to read unprompted emails and respond negatively to spam emails (2008, pp.764-765).

These findings with respect to gender and privacy are concordant with information about social network users overall; Caverlee and Webb found that women set their profiles to private more than twice as often as men, with younger users being more likely to have private profiles (Caverlee & Webb 2008). Fogel and Nehmad's study of 200 inner-city college students found that women were significantly more likely to express concern about online privacy and information disclosure on SNS. However, there is conflicting information about gender-based behavior. Boys are more likely to disclose personal information, take risks, and avoid privacy-protective behaviors (Steeves & Webster 2008, p.8; Fogel & Nehmad 2009, p.157), but another study showed that boys were more likely to post fake information on profiles than girls (64% to 50%) (Lenhart & Madden 2007, p.iii).

5.3 Age

There is an enormous difference in cognitive development, knowledge acquisition, and understanding between younger and older children. Z. Yan studied how 5-6 year olds, 8-10 year olds and 10-12 year olds conceptualized the Internet, and found that different age cohorts explained and understood the Internet in highly variable ways. He suggests that "children begin to understand the Internet as a complex artifact cognitively and socially during the 9-12 year old range" (Yan 2005, p.394). A follow-up study found that fifth and sixth graders have an adult understanding of the Internet's technical complexity, while social complexity is not grasped until 7th or 8th grade (Yan 2006). Given that the dominant discourse around young people and technology paints them either as naïve or sophisticated, it is striking that young teenagers understand the Internet as a socio-technical system in ways comparable to adults. Age was by far the dominant variable in predicting understanding of the Internet, more than frequency of Internet use, length of time online, or taking classes about the Internet (Yan 2006). This suggests that age is a significant variable in looking at all types of Internet use and comprehension among children and teenagers.

Therefore, it follows that privacy attitudes will differ by age. The likelihood of providing personal information online increases with age (Lenhart & Madden 2007, p.iv; Steeves & Webster 2008, p.8). Parents are less likely to monitor the Internet use of older teens, and regulated mediation loses its effectiveness with age, as 15-17 year olds tended to rebel against safeguards, filters, and the like (Lwin et al. 2008, p.213). Older teens were more likely to have their own Internet-enabled computer, and were more likely to visit adult chat rooms or pornographic sites (Steeves & Webster 2008, p.8). Although the Pew Internet project found that younger teens were more likely to post fake information than older teens (Lenhart & Madden 2007, p.iii), older teens were found to hold more sophisticated views of media literacy and subsequent greater concern over the potential of commercial websites to misuse personal information (Grant 2006).

5.4 Time Online

Teens who spend more time online are more concerned with privacy (Moscardelli & Divine 2007, p.243). This is consistent with Grant's typology of teenage attitudes, where the most Internet-savvy users were the most concerned with privacy and the most likely to engage in privacy-protective behaviors (2006).

5.5 Peers

The more a young person uses the Internet to talk to his or her friends and engage in playful, social behavior, the more likely that young person is to reveal personal information and the less likely to engage in privacy-protective behaviors (Steeves & Webster 2008, p.10). Youth with the highest levels of social confidence (e.g. popularity) were the most willing to divulge personal information, and the least likely to engage in privacy-protective behavior (Steeves & Webster 2008, pp.10-11). However, if a young person's peer group is concerned with privacy, he or she will most likely display greater concern as well (Moscardelli & Divine 2007, p.243; Moscardelli & Liston-Heyes 2004, p.53). Similarly, a study of 263 Australian teenagers found that "peer pressure" was a major motivator for revealing information on MySpace (De Souza & Dick 2009).

5.6 Website Safeguards

Website safeguards, which include content advisories, age verification, or credit card verification, were found to be reasonably effective at decreasing the amount of personal information provided by children 10-12 and 13-14; for 15-17 year olds, safeguards created a "boomerang effect" where teens reacted negatively, attempted to circumvent the safeguards, and ultimately tended to provide *more* personal information than when safeguards were absent (Lwin et al. 2008, p.213). (This effect disappeared with parental mediation).

5.7 Trust

Just like privacy, trust has been the focus of considerable academic debate related to privacy, digital technologies, and youth practices. Trust may be defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau et al. 1998, p.395). Despite conflicting theories about how trust is engendered and maintained, there appears to be consensus around a few key points: trust is empowering (and therefore, valuable) in many interactions, and while trust is most often developed over time, it can be lost quickly (Cullen & Reilly 2007).

Trust plays an important role in online interactions and relationships (Fukuyama 1996). Friedman, Kahn & Howe suggest that one primary difference related to trust in the online environment is the greater challenge individuals face in trying to reasonably assess the potential harm and goodwill of others (2000). An individual's ability to assess the trustworthiness of an organization is related to his or her expectations and knowledge of that organization, including the intentions and competence of the individuals who may be involved in any interaction that he or she has with the organization (Cullen & Reilly 2007). Furthermore, trust of a particular website or online social context is significantly related to information disclosure (Dwyer et al. 2007). For example, Facebook is consistently seen as more trustworthy than MySpace; as a result, Facebook members disclose more personal information than MySpace users (Fogel & Nehmad 2009; Dwyer et al. 2007).

Grant found that teenagers were concerned about the practices of online organizations, such as companies and website operators, who were viewed as untrustworthy (Grant 2006). Teenagers feared their personal information would be used without their permission for mailings, targeted advertising, or data-mining. The inability to tell how information provided online will be handled and used is referred to as “information risk” (Youn 2009). As a result, several of Grant’s informants reported that they did not trust the Internet as much as other media; he writes, “For the majority of young people in this research, feelings of deep skepticism towards commercial practices online dampened their overall enthusiasm towards Internet consumption” (p. 13). Similar findings have been reported by marketing research companies; Lindstrom found that 22% of teens stated that online privacy was the biggest reason they distrusted the Internet (Lindström 2001). Another study by Grant links young people’s mistrust of commercial practitioners with intrusive email, pop-ups, and poor understanding of the actual needs and wants of teens (Grant 2005, p.617).

Similar findings have been reported among adults. In a study of Singaporean adults, Xie et. al. found that the reputation of a company had a significant impact on whether or not a consumer would accurately reveal personal information to a commercial website (2006, p.71). Repeatedly, studies have shown that concerns over privacy increase when users do not know how their personal information will be used. Increased information risk thus increases the likelihood of a person adopting privacy-protecting behaviors (Youn 2009; Sheehan & Hoy 1999).

5.8 Culture and National Privacy Legislation

Historical events and traditions shape values and expectations (Cullen & Reilly 2007). Accordingly, there is an important relationship between people’s culture and their valuation and interpretation of privacy (Cullen & Reilly 2007, p.12). “There are many regional differences in how online privacy is treated in cultures around the world” (Palfrey & Gasser 2008, p.53). Various studies have confirmed that culture plays an important role in determining privacy concerns (Bellman et al. 2004; Cullen & Reilly 2007; Milberg et al. 1995); these concerns may impact the manner in which countries regulate information privacy.

Milberg et al. (1995) studied how people in different countries react to the collection, secondary use, errors, and improper access to personal information. They found that lower levels of information privacy concern are associated with countries with no privacy regulation, and/or countries with very strict privacy regulation. Higher levels of privacy concern will be associated with more moderate regulatory structures (Milberg et al. 1995). Differences in regulation reflect but also shape country differences (Bellman et al. 2004).

6. Disclosure of Personal Information

Disclosing personal information is often framed as a "risky" behavior and a potential privacy violation. Youth are seen at risk from marketers and companies who collect and sell personal data, and "online predators" and pedophiles (Palfrey et al. 2008). Personal information is a commodity that is bought and sold by data-mining companies like Choicepoint, marketing firms, and credit reporting agencies, and is especially valuable coming from young people, whose consumption is a multi-billion dollar industry (Xie et al. 2006; Moscardelli & Liston-Heyes 2004). Despite these warnings and fears, children and teens frequently share personal information online, whether by maintaining a profile on a social networking site, posting user-created content to sites like YouTube or DeviantArt, maintaining a blog or online journal, or talking over instant messenger or chat rooms. A 2007 study found that 64% of online teens and 59% of *all* teens had created online content (Lenhart et al. 2007).

However, providing personal information online does not inherently increase the risk of sexual solicitation. Although some studies have shown risks from providing certain types of personal information online—for instance, sharing names, pictures, and phone numbers in tandem with talking about sex with strangers has been linked to increased sexual solicitation (Wolak, Finkelhor, Mitchell & Ybarra 2008)—the majority of youth spend most of their time online talking to people they already know (Subrahmanyam & Greenfield 2008). A study of 1,500 Internet users ages 10-17 classified 17% of them as "high-risk unrestricted interactors"; the remaining 83% primarily interacted with people they knew in real-life or had been introduced to through friends (Wolak, Finkelhor & Mitchell 2008). Clearly, there is a difference in risk between providing personal information to a schoolmate or friend, and a stranger. Boyd and Schrock analyze these risks in some depth (2008).

It is also important to recall that there is no correlation between providing personal information online and a lack of concern for privacy; Tufekci's study of 700 college students found no relationship between concern for privacy and information disclosure on social network sites; students instead managed audience concerns through privacy settings and using obfuscating nicknames (Tufekci 2008). However, providing personal information can be linked to privacy in two ways. First, personal information provided in one context, such as a social discussion between peers, can flow to other contexts. For instance, a private instant messenger conversation can be cut-and-pasted and forwarded to other members of one's peer group, or a social network site profile can be mined for marketing information (Nissenbaum 2009). Second, the very act of providing information about oneself online, to a certain extent, makes this information "public," in that it is widely perceived as searchable and persistent. This perception is stoked by highly-publicized firings, evictions, and expulsions of college students and young adults for information posted on Facebook, MySpace or Twitter (Read 2006; Giffen 2008). In accordance with these incidents, "best practices" disseminated by colleges, institutions, and so forth strongly emphasize deleting or minimizing social network profiles, blogs, and other social media presences.

6.1 Risky Information

Hinduja and Patchin found that 18% of youth profiles indicated alcohol consumption, while 8% of profiles included information about smoking cigarettes and 2% smoking marijuana (Hinduja & Patchin 2008, p.136). A study of 147 MySpace profiles of 16-17 year olds found that 47% contained "risk behavior information," which the authors defined as sexual activity, alcohol use, cigarette use, and drug use—the most common was alcohol use, at 25% (Moreno et al. 2007). While these behaviors are not uncommon during adolescence, there is a worry that young people will be prosecuted or judged for this information, or that it will encourage others to engage in similar actions (Moreno et al. 2009).

6.2 Motivations

Discussions of children and teens disclosing personal information often take for granted that this provision is irrational or foolhardy. However, within the context of "real life" peer relationships, sharing personal information is normal and usual. This does not change for youth online. Maintaining a persistent identity ("nonymity") is necessary to engage in peer group discussions; sharing details and confidences can be ways to demonstrate trust between friends; and the desire to create and disseminate content may be linked to practices of "micro-celebrity", where attention is gained through self-conscious identity construction and forged relationships with others (Senft 2008; Marwick & boyd in review). Therefore, when weighing the risks, the benefits of sharing in online socializing must be considered.

Intimacy and Relationships

Youth use electronic communication primarily to reinforce pre-existing relationships (Subrahmanyam & Greenfield 2008; Boneva & Quinn 2006; E. F. Gross 2004; Moinian 2006). As a result, technologies like social network sites, mobile phones, and instant messenger play key roles in enforcing both individual friendships and peer group relationships. For instance, a study of children's online diaries in Sweden found that these self-presentations were "connected with other activities they do in their everyday life, and are in a dialogue with their social life, both at home and at school" (Moinian 2006, p.64). As a result, anonymity is not typical among adolescents, with the exception of role-playing gamers (Henderson & Gilding 2004). Although the use of real names is more common in environments like Facebook where a verifiable identity is required than in spaces like chat rooms, "nonymity", or a persistent identity, is common in much social media (Bechar-Israeli 1996; Zhao et al. 2008).

As previously discussed, sharing passwords or other private information can be a token of friendship and trust. Therefore, engaging in online behaviors that seem to violate "privacy" may be normative within a peer context. Children and teens may be motivated to post online content or discuss personal topics to increase intimacy with friends or place themselves within a peer sociality context. Valkenberg and Peter's study of intimacy over instant messenger concludes:

> We found a reciprocal relationship between intimate online self-disclosure and the quality of existing friendships. This result suggests an Internet-induced 'close-get-closer' effect: Adolescents who disclose more online develop higher quality friendships, and these same adolescents are in turn more inclined to disclose to these friends (2009, p.93)

Similarly, the use of social network sites, which require the sharing of personal information, allows young people to maintain weak ties, strengthen friendships, increase social capital and popularity (Ellison et al. 2007; Joinson 2008; Livingstone 2008; Christofides et al. 2009).

Identity

Posting information online can be a key part of identity play, expression, and formation (Moinian 2006; Subrahmanyam et al. 2004; Valkenburg & Peter 2008; Zhao et al. 2008). Even talking to strangers can be positive for youth, who may have concerns they cannot express to their "real life" peer group. For instance, for gay, lesbian, bisexual or transgender teens, talking to other gay-identified people can be an important source of support that combats isolation. A study of Dutch adolescents found that talking to strangers online, especially people of different ages and cultural backgrounds, positively affected their social competence. This was especially pronounced for lonely teenagers engaging in identity experimentation (Valkenburg & Peter 2008).

Microcelebrity

In her study of camgirls, young women using webcams to broadcast their lives to an online audience, Theresa Senft defines "micro-celebrity" as a technique that "involves people 'amping up' their popularity over the Web using techniques like video, blogs, and social networking sites" (2008, p.25). This practice is common among young people using social media creatively. Strategic micro-celebrity is distinct from the inadvertent fame resulting from Internet memes, such as the "Star Wars Kid" and "Tron Guy"; it involves viewing friends or followers as a fan base; acknowledging popularity as a goal; maintaining a fan base through contact with the audience and deliberate intimate disclosure; and strategically packaging and presenting oneself as a brand (Marwick & boyd in review).

Although micro-celebrity can be practiced by anyone of any age, publicized examples of micro-celebrity practitioners garnering mainstream attention tend to be young people. For example, teenage fashion bloggers like Tavi Gavinson, Jane Aldridge, and BryanBoy have been invited to fashion shows, covered by Vogue and Elle, and contacted by well-known designers (Gambrell 2009). Lucas Cruikshank, a 16-year old from Nebraska, gained recognition through YouTube; his popular character Fred Figglehorn is being turned into a film by a Hollywood studio (B. Barnes 2009).

However, the goal of micro-celebrity is not necessarily mainstream celebrity. Rather, it is status within a specific community, such as Harry Potter fans or crafters, or a particular site, like Twitter or Facebook. Since micro-celebrity is intrinsically about access—what differentiates the "micro" from the "celebrity"—the practice requires reaching out to interested readers and revealing personal information. This is supported by studies that show that online popularity is a major motivation for young people's use of social network sites (boyd 2007). A study of Canadian undergraduates found that popularity was a motivator for revealing personal information on Facebook; Christofides et. al write:

> It may also be the case that Facebook makes information disclosure the key factor in assessing a person's popularity. Having a presence on Facebook requires that a person post many pictures, have active discussions with friends, and share personal interests and information. Popularity and disclosure thus become inextricably linked… Disclosure thereby becomes an aspect of identity construction, and that construction is linked with popularity: the people who are most popular are those whose identity construction is most actively participated in by others. As a result, the risks of limiting access to personal information become greater than the risks of disclosure, because when limiting access, the individual also limits the potential for identity construction and thus potentially reduces his or her popularity (2009, p.343).

Although there is little empirical work on microcelebrity, the phenomenon of presenting ideal "possible selves" to an online audience has been documented in social network sites (Zhao et al. 2008) and online personals (Ellison et al. 2006; Gibbs et al. 2006). Compared to anonymous places like chat rooms, people displayed less of a discrepancy between "actual" and "ideal" selves in nonymous spaces, but people did tend to strategically emphasize positive aspects and craft a socially appealing profile (Gibbs et al. 2006). Similarly, two studies of identity construction on Facebook have found that people construct strategic identities that reflect their social milieus (Liu 2007; Zhao et al. 2008). Thus, the "micro-celebrity" identity presented to one's audience is likely to be constructed with the audience in mind, emphasizing qualities considered high-status within that community and de-emphasizing attributes that are not characteristic of their environment.

This process of playing an idealized, strategic self can be beneficial. Angela Thomas, in her ethnographic study of teenage Star Wars fan fiction authors, writes:

> Although I have so far discussed the ways in which the girls have both infused aspects of their "real" selves into their characters, the opposite is also true: the fictional characters are also a means for the girls to fashion new and emerging identities for themselves as they develop into adulthood. The characters allow the

> girls a freedom and power to author an identity…which plays out their fantasies and desires: of their physical bodies, their hopes and dreams for the future, and their ideas of romance. Their characters are a rehearsal of who they want to become, and in roleplaying that ideal self, they can grow closer to becoming that ideal (2007, p.160).

Although micro-celebrity does not necessitate playing an *idealized* self, the process of strategic identity construction allows for playful identity manipulation and trying different things out. Furthermore, the ability to gain status within an online community, particularly one that emphasizes creativity or skill, could be beneficial for a teenager; Ito et. al write, "…youth can gain status, validation and reputation among specific creative communities and smaller audiences… gaining recognition in these niche and amateur groups means validation of creative work in the here and now without having to wait for rewards in a far-flung and uncertain future in creative production" (2008, p.34).

7. Privacy Practices in Specific Sites

Perceptions of privacy and practices differ depending on the site. A website can be conceptualized as a context with its own specific set of privacy norms.

7.1 Commercial Websites

Uder United States law, the Children's Online Privacy Protection Act (COPPA, 15 U.S.C. § 6501–6506 (Pub.L. 105-277, 112 Stat. 2581-728, enacted October 21, 1998)) restricts the collection of personal information from children under 13, so most studies of commercial websites look at teenage use. As previously mentioned, an early study found that teens were more likely than adults to provide access to personal information to a commercial site in exchange for a free gift (Turow & Nir 2000). Youn found that teenagers were more likely to provide demographic information based on potential benefits, such as downloading music or accessing instant messenger. While teens were less likely to provide information if they perceived risk, they tended to underplay risk (2005). The context in which information is provided is very significant; a study of 3,000 Canadian children found that they were far more likely to provide their real name or address in exchange for a free e-mail address (76%), or on their own blog or website (57%), rather than in a chat room (5.9%) or a dating site (7%) (Steeves & Webster 2008, p.9).

7.2 Social Network Sites

Social network sites (SNS), such as MySpace, Facebook, Orkut, Bebo, and Hi5, are immensely popular among young people all over the world. In the United States, as of 2007, 58% of teenagers had created a profile on a social network site (Lenhart et al. 2007); among college students, this percentage was even higher. Jones and Soltren found that 91% of MIT undergraduates had a Facebook account (2005). "Social network" is a common term used to describe many different things; we use boyd and Ellison's definition:

> We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system (2007).

Social network sites are primarily used by young people to connect with friends they already know (Zhao et al. 2008; West et al. 2009; Lenhart & Madden 2007). Children and teenagers use social network sites to deepen intimacy, express themselves, engage in creative work, provide emotional support to others, learn more about people they have met in other contexts, and keep in touch with weak ties, such as far-away friends (Joinson 2008; Livingstone 2008). SNS have been shown to have many social benefits, such as increased social capital and popularity (Ellison et al. 2007). In fact, the social benefits and ritual use of SNS are so strong in some communities, especially among young people, that "the benefits… outweigh privacy concerns, even when concrete privacy invasion was experienced" (Debatin et al. 2009, p.100). Note that the majority of the studies cited in this section involve undergraduate students, whose use of SNS is very high and who are convenient samples for university-based researchers; there are few studies of younger teenagers and children's use of SNS (Livingstone 2008 is a notable exception).

Participating in social network sites, by definition, requires providing some sort of personal information in order to connect and communicate with other people. An early study by Gross and Acquisti of 4,500 Carnegie Mellon students on Facebook found that 90% of profiles contained an image, 89% a real name, 87.8% birthdate, and 50.8% their current residence and 40% a telephone number (Gross & Acquisti 2005). The Pew Internet and American Life project found that of teenagers with profiles on social network sites, 82% included a first name, 79% a photo, and 66% photos of their friends (Lenhart & Madden 2007). A study of 200 inner-city college students found that 86% displayed a photo on their profile, 81% their real name, and 83% information about interests and personality (Fogel & Nehmad 2009).

There are several contradictory studies about SNS and privacy. First, some researchers have found that Facebook users rarely change their privacy settings, leading to the conclusion that users are "quite oblivious, unconcerned, or just pragmatic about their personal privacy" (Valkenburg & Peter 2008; Acquisti & Gross 2006; Govani & Pashley 2007; Jones & Soltren 2005). For instance, the study of 200 inner-city college students found that 75% allowed anyone to view their MySpace or Facebook profile (Fogel & Nehmad 2009). However, other studies reach different conclusions; two-large scale studies concluded that slightly less than half of users set their social network profile to private, making it inaccessible to anyone outside their group of friends (Hinduja & Patchin 2008, p.138; Lenhart & Madden 2007), while a survey of undergraduates found that 69% had changed their Facebook privacy settings and half restricted their profile to friends-only (Debatin et al. 2009). Similarly, a survey of 350 Canadian undergraduates found that "students… were generally concerned about their privacy and reported that they were likely to use the range of privacy settings" (Christofides et al. 2009, p.343) as did a study of 700 American college students (Tufekci 2008). Generally, privacy protection on social networks is increasing over time, suggesting that the risks have been more publicized than in the past (Caverlee & Webb 2008; Lampe et al. 2008).

Second, it seems that many SNS users do not understand or read privacy policies or settings. While Jones and Soltren found that 74% of students were aware of Facebook's privacy options (Govani and Pashley cited 84%), the same researchers found that 89% of users had never read the privacy policy and 91% were unfamiliar with the Terms of Service (H. Jones & Soltren 2005; Govani & Pashley 2007). However, Govani and Pashley found that increased awareness of privacy settings did not affect information provision, suggesting that ignorance of privacy settings is not wholly responsible for the reluctance of students to restrict access to their profiles (2007). Debatin et. al. conclude that "while a majority of Facebook users report having an understanding of privacy settings and make use of their privacy settings, it is also apparent… that they may have a skewed sense of what that exactly entails" (Debatin et al. 2009, p.100).

Third, "personal information" consists of many different information types, which are considered more or less private. The same Pew Internet and American Life study previously cited noted that only 2% of profiles listed telephone numbers, and only 11% both first and last names. Hinduja and Patchin's quantitative study of MySpace found that 8.8% revealed a full name, 57% a picture, 28% a school name, and less than 0.3% a phone number (Hinduja & Patchin 2008, p.125). Similarly, Fogel et. al. found that less than 10% of users included a phone number and 9.4% a home address (2009, p.156).

Fourth, some studies have found young people to be *more* privacy-conscious on SNS than older users. For instance, the Pew Internet Project found that teenagers were more likely to restrict access to SNS profiles and shared photos than adults (Lenhart et al. 2007) (see "Privacy-Protecting Behavior" for more). The way that young people use SNS seems consistent with *all* social media users. For instance, 99.9% of MySpace users of all ages were found to show some age, gender, or location information, but younger users were found to be more likely to adopt a private profile than older users, perhaps due to increased tech-savviness in younger groups (Caverlee & Webb 2008).

However, there are several other layers of potential privacy violations on social network sites like Facebook and MySpace. First, employers, law enforcement, government agencies, school districts, insurance companies, and corporations can and do use social network sites to collect information about prospective hires, potential law-breakers, criminal acts, students, risky behaviors, and consumer behavior (Debatin et al. 2009; Marwick 2009). Social network sites can be subpoenaed by a government agency to provide account information, even if that account is locked based on privacy settings. Recently, the *New York Times* called for the United States government to answer a Freedom of Information Act request for the extent of law enforcement requests for social media site information (The New York Times 2009). There are no current regulations in the United States protecting social network users from this type of information collection and surveillance, even in instances where similar data-collection *offline* would be illegal (for instance, investigating the race of a potential interview subject), unless such surveillance were to violate the terms of service or the privacy policy to which the user and the site had agreed.

Second, many social network sites profit from the sale of personal information, using behavioral marketing to target advertising, track user behavior across websites, and allow third-party

applications to access private information from users and their friends (Jones & Soltren 2005; Debatin et al. 2009).
young people's lives that their benefits almost always outweight the risks. Debatin et. al conclude: "safer use of social network sites would thus require a dramatic change in user
However, as previously stated, SNS are such a highly-integrated part of many attitudes: a responsible and informed user with a high degree of computer literacy—not just in the technical but in the sociocultural and ethical sense, as well" (Debatin et al. 2009, p.102).

7.3 Instant Messenger

Instant messenger (IM) is a very popular method of communication among children and teenagers, who primarily use it to talk to their "real-life" friends (Boneva & Quinn 2006; Valkenburg & Peter 2009; E. F. Gross 2004); 68% of teens who use the Internet use instant messenger (Lenhart et al. 2007). Gross found that 84% of IM conversations occurred with people the user had met before going online, and 82% were friends from school (2004, p.642). A study that included both qualitative interviews and a telephone survey with 96 teens found that instant messenger was used both to reinforce one-on-one friendships and peer group maintenance (Boneva & Quinn 2006). Both Gross and Boneva concluded that IM serves a similar function to the telephone, in that IM helps to maintain pre-existing relationships. A recent study of 812 Dutch teenagers found that ongoing IM use with friends increased friendship ties; the researchers concluded that this positive effect "could be explained entirely by adolescents' tendency to disclose intimate information online" (Valkenburg & Peter 2009, p.79).

Because so many sensitive conversations go on over IM (gossip, relationships, dating, personal conversations, etc.) young people are highly aware of the potential for IM conversations to be copied or distributed (Grinter & Palen 2002; Patil & Kobsa 2005). A qualitative study of 16 IM users found that teenagers wanted access regulation "to keep strangers as well as particular peers away," and that they used IM features in sophisticated ways to protect their privacy or avoid being interrupted. This included not engaging in public chat, keeping profiles private, and publicizing their reasons for prolonged absences (Grinter & Palen 2002).

7.4 Blogs

According to the Pew Internet and American Life project, 28% of teens have started a personal journal or blog (Lenhart et al. 2007). Studies of youth bloggers show that personal information, such as name, age, location, and contact information, is frequently revealed on personal blogs (Huffaker 2006; Huffaker & Calvert 2005). These findings are consistent with Viégas' study of privacy attitudes among adult bloggers, which showed that 81% of participants provided some form of self-identification (2005).

7.5 Mobile Phones

As of 2008, the Pew Internet project found that 77 % of American teens had a mobile phone. Older teens are more likely to have their own cell phone; 53% of 12-13 year olds own a mobile, while 84% of 17 year olds owned one (Lenhart 2009). Ownership is even higher in Europe, where the average mobile penetration rate is 104%, or more than one cellphone per person (Grant & O'Donohoe 2007).

Mobile phones are overwhelmingly seen as private spaces. Teenagers see commercial use of mobile technologies, such as advertising via text message, as an unwelcome intrusion into a personal, private space (Grant & O'Donohoe 2007, p.240). A study of 175 Scottish teenagers found that the mobile phone was seen as a more private form of communication than the Internet; texting, especially, was a way to talk to friends without eavesdropping from parents, teachers, or classmates (Grant & O'Donohoe 2007). A similar study of British families found that only a small minority of teeenagers did not mind their parents checking their phones; most parents viewed the phone as a “diary” and never or rarely looked at their children’s cell phones (Devitt & Roker 2009). For children, cellphones are often described in a language of independence and empowerment (Campbell 2006). They allow private communication with friends, particularly conversations with people that are not easily had at home (estranged relatives or friends their parents do not approve of). They may also allow greater mobility for children. However, many parents see cellphones as a “digital leash” which makes it possible to contact their children at any time, contributing to peace of mind but also greater surveillance (Devitt & Roker 2009; Fotel & Thomsen 2004; Pain et al. 2005).

7.6 Video Games

Games are very popular with young people; the Pew Internet project found that “by a large margin, teen Internet users’ favorite online activity is game playing; 78% of 12-17 year-old Internet users play games online” (Jones & Fox 2009). Although console games, casual games like solitaire and Bejeweled, and networked games like Xbox Live and World of Warcraft generally collect and store information about users, there is little work on the extent of this information collection or how young people respond to it. A few researchers in the game studies field have investigated how technologies of surveillance are being incorporated into video games, both to track player metrics and to mimic the aesthetics of surveillance in gameplay (Albrechtslund & Dubbeld 2005; Taylor 2006).

8. Privacy-Protecting Behaviors

Studies of teenagers coping with risk have found two broad strategies: *approach strategies*, which consist of problem-solving, information-seeking and support; and *avoidance*, which uses distance and defensive mechanisms. A study of adults found similar overall strategies for dealing with privacy: *confrontive* (approach) and *avoidance* strategies (Raman & Pashupati 2005). Among children and teenagers, approach strategies include falsifying personal information, asking parents or teachers for advice, and reading privacy statements, while avoidance includes refusing to use certain websites (Youn 2009). Privacy-protecting behaviors include obfuscation, refusal to provide information, provision of false information, maintenance of multiple profiles on social media sites, flaming, circumventing age restrictions, and so forth.

Studies have found that teens are *more* vigilant than adults in terms of privacy-protecting behaviors, although they are more likely to engage in "less ethical" approaches like flaming and providing false information (Moscardelli & Divine 2007, p.246; Lenhart et al. 2007; Caverlee & Webb 2008). Teens are more likely to engage in privacy-protecting behaviors if they are concerned with privacy, perceive information risk, or see themselves as vulnerable (Youn 2009). However, a study of 547 teenagers found that teens often see themselves as able to circumvent threats; a high perception of self-efficacy may mitigate the effect of increased risk perception (Wirth et al. 2007). Often, youth engage in these behaviors primarily to protect their privacy from parents, peers, or teachers (Subrahmanyam & Greenfield 2008, p.124).

8.1 At Home

Livingstone observed various strategies children used to maintain their privacy from parents while accessing email, chat rooms, and web pages in the home. Using multiple e-mail addresses and instant messenger/chat room accounts, writing messages to peers in text-speak, and usage of passwords and window minimization represent "boundary marking tactics," the equivalent of a "keep out!" sign on a bedroom door (Livingstone 2006). The Digital Youth Project found that teenagers developed "work-arounds and back channels" to hang out with each other even when schools and parents put measures in place to prevent this (Ito et al. 2008). Qualitative studies have found evidence that children enjoy outwitting adult attempts to filter websites or monitor Internet usage (Ito et al. 2008; Hope 2007; Hope 2005; Livingstone 2006). Accessing "forbidden" sites like jokes, pirated music, or pornography can also be a way for young people to assert freedom or privacy while surfing the Internet (Livingstone 2006). The Internet, particularly chat rooms or spaces like Facebook and MySpace, may function as *private* spaces for children who are highly regulated and observed in their family and school life (boyd 2008).

8.2 Surveillance

Children resist both direct and remote surveillance in a variety of ways, circumventing monitoring technologies and engaging in “sousveillance” (watching the watchers). A study of eight schools in the United Kingdom, including 63 interviews, found that students circumvented Internet monitoring by concealing their Internet activity physically (in remote classrooms, with their monitors turned to the side, or rapidly-closing windows) and virtually (sharing passwords, accessing innocuous-sounding websites for purposes that would be deemed unsuitable). Even knowing that Internet access was tracked and monitored did not necessarily deter students, who assumed that the volume of tracking information would be too great for administrators to carefully parse (Hope 2005). A qualitative study of Scottish youth found that several children reported “regularly subverting, challenging and renegotiating parental controls” over mobility (Backett-Milburn & Harden 2004, p.437). Similar studies in Northeast England found that some of the features of mobile phones that make them unreliable for remote surveillance (battery life, out of range, etc.) were used by children as excuses for not getting in touch with anxious parents (Pain et al. 2005, p.821).

8.3 Falsifying Information

To cope with commercial websites asking for personal information, Youn found that 53% of her sample (326 Midwestern high school students) provided incomplete information, 44% gave out false information such as a fake name, 43% left the site without providing information, and the same amount went to other websites that did not require the provision of personal information (2005, p.99). Moscardelli and Divine, in a study of 700 Midwestern high school students, found that students concerned about privacy most often responded by providing inaccurate or false information and requesting to be removed from e-mail lists (2007, p.244). Similarly, an ethnographic study of 175 Scottish teens found that providing false information was seen as a way to resist overly intrusive marketing and advertising practices (Grant 2006). In social network site profiles, the Pew Internet project found that 46% of respondents falsified information on their profiles, both to protect themselves and be funny or playful (Lenhart & Madden 2007, p.ii). However, a study of 175 American seventh-graders found that younger children were not likely to falsify information, despite the prevalence of this practice among older teenagers and adults. Youn speculates that 10-12 year olds are unused to providing false personal information, or are less savvy about the benefits of anonymity online (Youn 2009).

8.4 Reading Privacy Policies

Most youth do not read privacy policies, and when they do, rarely act on that information. Youn found that 36% of her sample (326 Midwestern high school students) read a site’s privacy policy when asked for personal information, while 23% asked a parent or teacher how to manage risk. More experienced users were more likely to read privacy policies, while younger teens were more likely to ask for advice (2005, p.99). A study of more than 3,000 Canadian 13-17 year olds found that 48.9% of youth had never read a site's privacy policy and those who had did not necessarily change their behavior accordingly (Steeves & Webster 2008, p.8).

8.5 Identity Play

Some children and teenagers have engaged in identity play online (pretending to be someone other than themselves). Gross found that about half of the 175 7th and 10th graders in her survey had pretended to be someone else online, but of that, almost all had pretended to be older, possibly to access websites not available to younger people (2004, p.643). Steeves & Webster found that the majority (59%) of their 3,000 respondents had, at one time, pretended to be a different age (52%), a different personality (26%), or someone with a different physical appearance (23%). Respondents said they did this for a variety of reasons, including seeing what it would be like, to flirt, to pretend to be older, or to act "mean" (Steeves & Wing 2005, p.10). Identity play correlated to the increased relevalation of personal information online – i.e., the more the Internet was used to play with identity, the more likely the youth was to reveal personal information (Steeves & Webster 2008, p.12).

8.6 Changing Privacy Settings

Although changing privacy settings on social media sites like Facebook or MySpace is often difficult or confusing for teenage users, studies show that this is becoming more common (Livingstone 2008, p.406). While Gross and Acquisti found that very few Facebook users changed their privacy settings, a longitudinal study by Lampe and Ellison found that in 2006, 64% of users kept the default privacy settings, which dropped to 45% in 2007 and 48% in 2008 (R. Gross & Acquisti 2005; Lampe et al. 2008). The Pew Internet and American Life project found that 66% of teenage social networking site users limited access to their profiles in some way (Lenhart & Madden 2007, p.ii). (See the section on social network sites for a comprehensive review of studies on this topic.)

Across social media types, children and teens set stricter privacy restrictions than adults (Moscardelli & Divine 2007; Lenhart et al. 2007; Caverlee & Webb 2008). For example, the Pew Internet Project found that 39% of teenagers who posted photos online restricted access "most of the time" and 38% "sometimes," while only 21% "never" restricted access. Among adults, "34% restrict access most of the time, 24% some of the time, and 39% say they never restrict access to online photos" (Lenhart et al. 2007, p.iii).

9. Regulating Privacy

The governance of privacy is exercised through diverse institutional forms—including public and private, domestic and transnational. As a result, government regulators are not always the most important actors, nor the laws they enact the most important privacy-protective instruments. Self regulatory approaches take on significance as a result (Bennett & Raab 2006). Culture plays an important part in shaping privacy claims and norms (Cullen & Reilly 2007). Accordingly, there are differences between countries regarding each country's privacy environment, ranging from their regulatory environment to privacy's role in society, and the legislative approaches used to address privacy issues. For example, while the United States has taken a sectoral approach to regulating privacy, many of the states elsewhere in the world have enacted omnibus information privacy laws, including all member nations of the European Union (Solove & Schwartz 2009). However, any single comparison between countries is impossible because of the many different policy areas and policy instruments throughout the world (Bennett & Raab 2006).

9.1 Fair Information Practices

The concept of Fair Information Practices, like the development of a legal right of privacy, is an American conception (Rotenberg 2001). From the mid-1960s to the mid-1970s, the growing threats to privacy from technology emerged as central political and social concern in the United States (Solove et al. 2006). Philosophers, legal scholars, and others turned their focus on how technological advancement allowed larger and larger amounts of personal data to be aggregated and distributed more quickly and efficiently than most people thought possible prior to this period (Ciocchetti 2007). Governmental and private groups began searching for a list of values critical to the protection of an individual's information privacy (Ciocchetti 2007). This led to various policy statements—commonly referred to as statements of fair information practices, which seek to ensure the fair collection and use of personal information, not the open-ended regulation of technology (Rotenberg 2001). Not only Fair Information Practices have played a significant role in framing privacy laws in the United States and around the world, they also contributed to the development of important international guidelines for privacy protection (Rotenberg 2001).

In 1973, the U.S. Department of Health, Education and Welfare (HEW) developed the Code of Fair Information Practices (HEW 1973). The HEW Code attempted to establish fairness in the automated collection and handling of personal information through adherence to the following five fair information principles: (1) Openness; (2) Disclosure; (3) Secondary Use; (4) Correction; and (5) Security. Upon its release, the principles of the HEW Code became fairly well accepted in the business and international communities (Ciocchetti 2007). The international community was simultaneously interested in fair information practices and issued separate statements with similar fair information practices principles. Seven years later, the Organization for Economic

Cooperation and Development (OECD) issued the most well known guidelines developing the concept of fair information practices: the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD 1981). The OECD Guidelines set out eight principles for data protection: (1) Collection Limitation; (2) Data Quality; (3) Purpose Specification; (4) Use Limitation; (5) Security Safeguards; (6) Openness; (7) Individual Participation; and (8) Accountability. The OECD Guidelines have served as a benchmark for assessing privacy policy and legislation (Rotenberg 2001).

9.2 Youth Privacy Protection in the United States

Although the codes of fair information practices developed since the 1970s have been influential, the United States Congress has not passed comprehensive federal legislation requiring consistent application of fair information practices to the collection, use, storage, or dissemination of personal data by private entities (Ciocchetti 2007). Instead, the United States government has incorporated certain fair information practices into various sectoral regulations and left others to be enforced by governmental agencies or incorporated into industry self-regulation efforts (Ciocchetti 2007; Cullen & Reilly 2007; Rotenberg 2001; Stanaland et al. 2009). This sectoral approach has resulted in the development of different privacy codes for various areas (e.g. the Health Insurance Portability and Accountability Act of 1996, the Family Educational Rights and Privacy Act, the Fair Credit Reporting Act, Electronic Communications Privacy Act of 1986, among others). Various authors point out the ineffectiveness of this sectoral regulatory approach. Rotenberg, for example, argues that the coverage of U.S. law is uneven: fair information practices are in force in some sectors and not in others (2001, p.48). Generally, there is an inadequate enforcement and oversight because technology continues to outpace the law (Mills 2008; Rotenberg 2001).

In a self-regulatory context, fair information practices define the privacy rules (Stanaland et al. 2009, p.477). In general, the FTC has encouraged businesses to address consumers' concerns for online privacy issues through self-regulation and adherence to what they consider the five core principles of fair information practices (Federal Trade Commission 1998):

> *Notice/Awareness*: Consumers should be given notice of an entity's information practices before any personal information is collected from them. Notice to the consumers in the Internet can be accomplished by posting an information practice disclosure but it has to be clear, conspicuous, and readily accessible to Internet users.
>
> *Choice/Consent*: Choice or consent relates to the availability of options provided to consumers particularly in respect to how any personal information that is collected from them is subsequently used by the entity collecting the information. This is to allow consumers to decide whether to disclose personal information

> especially when the information collected may be used for purposes beyond those necessary to complete the contemplated transaction.
>
> *Access/Participation*: Access or participation refers to the ability of an individual to both access the personal information about him or herself and contest the information's accuracy and completeness. The objective of this fair information practice is to ensure that data are accurate and complete.
>
> *Security/Integrity*: This fair information practice principle ensures that the entity engaged in data collection takes reasonable steps to assure data integrity and to protect data against loss, unauthorized access, destruction, and use or disclosure of the data. Like the previous principle of access or participation, the objective of the security or integrity principle is to ensure data accuracy and completeness.
>
> *Enforcement/Redress*: As with all rules and regulations, the core principles of fair information practices can only be effective if there are enforcement mechanisms or avenues of redress when the principles are not complied with or breached. Enforcement measures may take the form of self-regulation, private remedies, or government enforcement (Stanaland et al. 2009, pp.477-478).

These principles allocate rights and responsibilities in the collection and use of personal information. However, because these principles function primarily as recommendations for maintaining privacy-friendly data collection practices, their adherence and enforcement is exclusively self-regulatory. As a result, US-based websites aggressively collect personal information from their visitors (Stanaland et al. 2009) with virtually no fear of reprisal from the state. "Under this self-regulatory model, the burden of protecting consumers' online privacy essentially falls back on the individual consumer who must assess the trade-off between safeguarding one's privacy and the convenience of the commercial online transactions" (2009, p.478).

9.3 Children's Online Privacy Protection Act

Although the United States follows loose guidelines in terms of overall privacy, the federal government enforces strict requirements in terms of children's online privacy (Stanaland et al. 2009, p.479). Aware of businesses' practices of collecting children's personal information and the risks such practices signify, the United States Congress enacted the Children's Online Privacy Protection Act (COPPA) on October of 1998[1] to regulate the online collection of personal information from children under thirteen by persons or entities under U.S. jurisdiction (1998). COPPA only applies to companies operating websites directed to children under the age

[1] 15 U.S.C. §§ 6501–6506 (2006).

of thirteen or to companies operating general-audience websites that have "actual knowledge" that they are collecting personal information from children under thirteen.[2] COPPA defines personal information as individually identifiable information about an individual collected online, including first and last name, address, e-mail address, telephone number, Social Security Number, any other identifier that the FTC determines that permits the physical or online contacting of a specific individual.[3]

COPPA does not require websites to verify the age of all its visitors. Nevertheless, websites must obtain parental consent prior to the collection of personal information from children under thirteen and post an electronic privacy policy that explains: (1) the types of personal information collected from children;[4] (2) whether such information is obtained actively or passively;[5] (3) how this information will be used;[6] (4) whether the information will be disseminated to third parties;[7] and (5) that a parent may review and delete a child's personal information and refuse to consent to additional collection.[8] The privacy policy must also contain contact information pertaining to the operators of the website so that parents have the opportunity to contact these administrators with questions or comments. This contact information must include the: (1) name; (2) mailing address; (3) telephone number; and (4) e-mail address of all operators maintaining personal information from children obtained through the website.[9]

Pursuant to COPPA, websites must contain at least a hyperlink to the electronic privacy policy that must be placed in a clear and prominent place on the website home page and at all places where children may be required to submit personal information.[10] COPPA defines a clear and prominent hyperlink as one where the text of the link is in a different color, type size, or font from the text located on the rest of the webpage where such hyperlink resides.[11] COPPA also requires that privacy policies be written in language that is clear and understandable.[12] Concerning enforcement, violations of COPPA may be treated as unfair or deceptive acts and/or practices prohibited under the FTC Act and enforced by the FTC. COPPA preempts any state or local law that would conflict with its provisions, but allows state attorneys general to initiate civil actions based on COPPA violations and serve in the place of parents over the course of such lawsuits.[13]

[2] 15 U.S.C. § 6502(a)(1).
[3] 15 U.S.C. § 6501(8).
[4] 15 U.S.C. § 6502(b)(1)(A)(i); 16 C.F.R. § 312.4(b)(2)(ii) (2006).
[5] 16 C.F.R. § 312.4(b)(2)(ii).
[6] 15 U.S.C. § 6502(b)(1)(A)(i); 16 C.F.R. § 312.4(b)(iii) (2006).
[7] 15 U.S.C. § 6502(b)(1)(A)(i) and 16 C.F.R. § 312.4(b)(2)(iv) (2006).
[8] 16 C.F.R. § 312.4(b)(2)(vi) (2006).
[9] 16 C.F.R. § 312.4(b)(2)(i) (2006).
[10] 16 C.F.R. § 312.4(b) (2006).
[11] *Id.*
[12] *Id.*
[13] 15 U.S.C § 6504(a)(1).

COPPA functions in the marketplace in such a way as to give children's online privacy in the United States a "high standard of protection" (Bartoli 2009, p.7). For example, the required disclosure of how children's personal information will be used and whether it will be disseminated to third parties disclosures give parents the opportunity to understand the privacy obligations related to the submission of their children's personal information (Ciocchetti 2007, p.77). COPPA's preemption clauses are valuable because "they disallow conflicting laws allowing businesses to comply with only one federal law concerning children's online privacy rather than a multitude of potentially conflicting state laws" (Ciocchetti 2007, p.77). Also, since both the FTC and state attorneys general can enforce COPPA provisions more resources can be aimed at protecting children's personal information (Ciocchetti 2007, p.77).

Criticisms of COPPA

COPPA has been criticized for a number of reasons. COPPA's age limit (thirteen) has been classified as arbitrary because children's development, being a process not a race, makes it difficult to establish the precise age at which they can make an informed decision to provide businesses with their personal data (Bartoli 2009, p.38). Children also provide a false age to web sites in order to access general audience websites (Bartoli 2009). According to the FTC, the proliferation of general audience websites that may appeal to younger audiences "highlights the need for supplemental solutions, such as age verification technologies, that can provide additional measures of security for children as they increasingly engage in online activities" (2007, p.3).

COPPA interposes parental involvement in their child's electronic interactions by requiring parental consent for the collection of a child's personal information; ensuing regulations initially relied on the promise of emerging technologies to aid parents in this endeavor (Hiller et al. 2008). COPPA's parental consent formulation has been criticized for being unrealistic, costly, and more beneficial to businesses than to parents (Hiller et al. 2008).

The two procedures proposed to establish the authenticity of the parental consent to the collection of the child's personal data are: (1) sending an e-mail; and (2) provision of the parents' credit card details (Bartoli 2009; Hiller et al. 2008). Since children can easily get this information, there is no way to know if the consent provided is genuinely from a parent (Bartoli 2009). According to Hiller et al., parental consent methodologies and effectiveness have not been studied or analyzed (2008). Instead, the FTC anticipated the evolution of a technological solution to more powerfully and effectively support this element of the law; however, that never materialized, leaving regulations setting standards for parental consent to be limited to the same methods as those available in 2000 (Hiller et al. 2008).

Pursuant to COPPA, parents have the right to review and delete the data collected from their children by the websites. Implementing the provisions relating to the deletion of children's data might be problematic since there are numerous situations in which websites owners ought to retain children's personal data (Bartoli 2009). This is the case where litigation is threatened or pending, where a law enforcement investigation is ongoing or where the information is necessary to detect or prevent unlawful activity (Bartoli 2009). Parental control over the data collected from their children raises another issue: "how to balance children's privacy and the needs for parents to control what their children do online" (Bartoli 2009).

9.4 Federal Trade Commission

Companies operating websites that fall outside COPPA's jurisdiction but still target young people remain under the watch of the FTC, which has the authority to enforce the commitments made to Internet users under privacy policies under the FTC's general unfair and deceptive practices powers. Since 1998, the FTC has maintained the position that the use or dissemination of personal information in a manner contrary to a posted privacy policy is a deceptive practice under the FTC Act (Solove & Schwartz 2009). Although the FTC does not require companies to post privacy policies, it has the authority to bring an enforcement action as either an unfair or a deceptive practice, or both, if promises are made and subsequently broken. Section 45(a)(1) of the FTC Act prohibits unfair and deceptive acts or practices in interstate commerce. An unfair or deceptive act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition".[14] The FTC is allowed to exercise its general enforcement authority if: (1) it has reason to believe that an unfair or deceptive act or practice is occurring and (2) if it appears to the FTC that bringing an action is in the public interest.[15] The FTC Act authorizes the FTC to bring civil actions for penalties up to $10,000 for a knowing violation of the Act.[16]

Under its unfair practices authority, the FTC has brought several cases, most of which has settled, involving the breach of a promise made in an electronic privacy policy (Solove & Schwartz 2009). The typical situation in which the FTC has brought deceptive practice actions involves a data security breach incident where a company's promise of data security was not implemented or improperly monitored. The FTC has also brought enforcement actions where no privacy promises were breached, in situations where companies fail to adequately protect personal information. For example, the FTC brought an unfair practices action against BJ's Wholesale Club, Inc. for failure to employ reasonable and appropriate security measures to protect personal information by not encrypting such information in transit, storing it in places where it could be accessed anonymously, failing to limit network access through wireless access points, failing to employ sufficient measures to detect unauthorized access, and storing information for longer periods than necessary.

[14] 15 U.S.C. § 45(n).
[15] 15 U.S.C. § 45(b).
[16] 15 U.S.C § 45(m)(1)(A).

Many states in the United States have analogous statutes to the FTC Act with respect to unfair and deceptive trade practices. For instance, chapter 93A of the Massachusetts General Laws regulates business activity in order to protect consumers from unfair and deceptive trade practices.

9.5 Canada

Canada has two federal privacy laws: the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Since 1983, the Privacy Act regulates the government's collection, use and storage of personal information.[17] Under its provisions, such information should be: (1) collected by government institutions in relation to operating programs or activities; (2) collected from the individual personally; (3) accurate and up to date; (4) subject to correction by the individual; and (5) used only for the purpose for which it was originally collected. PIPEDA[18] is the main legislation governing the collection, storage and use of personal information in the private sector, including telecommunications companies, Internet service providers and companies that conduct business online (Canadian Working Group 2009; Solove & Schwartz 2009). Both the Privacy Act and PIPEDA are overseen by the Privacy Commissioner of Canada, which has the authority to investigate complaints by individuals and to conduct audits.

PIPEDA extends to all personal information used in connection with any commercial activity (§ 4(1)-(2)). Under PIPEDA, organizations which commercially use personal information, or make other exempt uses of it, are required to follow ten fair information practices principles, which are modeled on the OECD Guidelines, but mostly on the Canadian Standards Association Model Code for the Protection of Personal Information (Solove & Schwartz 2009). The principles are: (1) accountability— organizations are responsible for the personal information under their control and must designate an individual or individuals who are accountable for the organization's compliance with these principles; (2) identifying purposes—before or at the time the information is collected, the organization must disclose the purposes of such collection; (3) consent—individuals must know about and consent to the collection, use or disclosure of their personal information, except when inappropriate; (4) limiting collection—to that which is necessary for the purposes identified by the organization; (5) limiting use, disclosure and retention—to the purposes for which the information was collected, except with the consent of the individual or as required by law; (6) accuracy—the personal information must be as accurate, complete and up-to date as is necessary for the purposes for which it is to be used; (7) safeguards—the organization must establish appropriate security safeguards to protect the information; (8) openness—information regarding the organization's policies and practices on the management of personal information must be readily available to individuals; (9) individual

[17] R.S., 1985, c. P-21.

[18] 2000, c. 5, P-8.6.

access—upon request, an individual must be informed of the existence, use and disclosure of his/her personal information and must be given access to that information. Individuals must be able to challenge the accuracy and completeness of the information and have it amended as appropriate; and (10) challenging compliance—an individual must be able to address a challenge concerning compliance of these principles to the individuals designated by the organization (PIPEDA at Schedule 1).

PIPEDA requires organizations to obtain consent from the individual in order to collect, use or disclose their personal information. However, this consent-based model of protection "does not look at the relative maturity or age of the person offering consent, nor are the standards for ensuring the consent is informed sufficient. To put it simply, children are not differentiated from adults when considering their privacy rights" (Canadian Working Group 2009, pp.16-17). The Privacy Commissioner "has been nearly silent in interpreting this Act in the light of the collection, use and disclosure of information from children, probably due mostly to the fact that the Office is complaint-driven, and not many parents have taken the time to complain on behalf of their minor children" (Public Interest Advocacy Center (PIAC) 2008, p.50). In their 2008 report, the Public Interest Advocacy Centre (PIAC) concluded that Canada's legislative framework is insufficient to protect children's online privacy and recommended that PIPEDA be amended to add specific rules to protect children's online privacy. PIAC proposed a scheme of varying consent requirements:

1. Under thirteen: a general prohibition on the collection, use and disclosure of all personal information.

2. Aged 13 – 15: websites would be permitted to collect and use personal information solely in relation to that website with the explicit consent of the teen and parent and would not be permitted to further disclose their personal information.

3. Aged 16 to legal majority (18 or 19): websites would be permitted to collect personal information with the teen's consent, and disclose the personal information of the teen only with the opt-in consent of the teen and explicit consent of a parent.

4. After attaining the age of majority: websites and corporations would no longer be permitted to retain the information gathered when the child was below the age of majority and would be required to delete the information immediately without the explicit consent of the person attaining the age of majority.

A number of Canadian industry associations have enacted voluntary privacy codes. In 2004, the Canadian Marketing Association (CMA)—the largest marketing association in Canada—updated its Code of Ethics (CMA Code) to include provisions regarding the marketing to children and teenagers. For purposes of the CMA Code, a child is someone who is under thirteen (K1), while a teenager refers to "someone who has reached their thirteenth birthday but has not yet reached the age of majority in their province or territory of residence" (L1). The CMA Code requires that "all marketing interactions directed to children that include the collection, transfer and requests for personal information require the opt-in consent of the child's parent or guardian" (K3.1). If for some reason "the child, parent or guardian withdraws or declines permission to collect, use or disclose a child's information, marketers must immediately delete all such information from their database" (K3.2).

Marketers must obtain opt-in consent from teenagers between the ages of thirteen and sixteen for the collection and use of their contact information (L3.1). However, marketers must obtain the opt-in consent of their parent or guardian before disclosing such information to a third party (L3.1). For the collection, use or disclosure of personal information that exceeds contact information belonging to a teenager under sixteen, the opt-in consent of their parent or guardian must be obtained (L3.1). For teenagers over the age of sixteen but below the age of majority, marketers must obtain the teenager's opt-in consent for the collection, use and disclosure of their personal information (L3.2). However, where the teenager, parent or guardian withdraws or declines permission to collect, use or disclose a teenager's personal information, the marketer must immediately delete all such information from their database (L3.3). Additionally, the CMA Code stresses that marketers must use age-appropriate language and imagery in their advertisements (K6, L6).

The CMA Code has some noteworthy privacy-enhancing requirements. First, it tailors its privacy requirements according to children's age and presumed maturity level. Second, it gives parental control over disclosure of personal information of their children. On the downside, because the CMA Code is voluntary, it is not legally enforceable, but by virtue of their membership, every company that belongs to the CMA is bound to the CMA Code (Canadian Marketing Association 2009, sec.D1)

9.6 Youth Privacy Protection in Europe

In Europe, the protection of individuals with regard to the collection, processing, use and movement of personal data is covered by the European Parliament and Council Directive 95/46/EC of October 24, 1995, or the Data Protection Directive (Directive 95/46/ec of the European Parliament 1995). The Data Protection Directive came about in response to the economic requirements of the integration of the European national markets in the early 1990s (Solove & Schwartz 2009; Rotenberg 2001). The processing of personal data and the protection of privacy in the electronic communications sector are the subject of Directive 2002/58/EC of the

European Parliament and of the Council of July 12, 2002, or the Directive on Privacy and Electronic Communications (Directive 2002/58/EC of the European Parliament 2002). This Directive extends privacy protections to unsolicited commercial e-mail, telephone communications, requires websites to disclose the use of cookies, and recommends that privacy notices are short and easy for consumers to understand. Since neither the Data Protection Directive nor the Directive on Privacy and Electronic Communications distinguish between data subjects who are adults, children or teenagers, they do not provide specific protection for youth privacy.

The Data Protection Directive takes a more comprehensive approach to privacy protection in the private sector than the United States does (Solove & Schwartz 2009; Rotenberg 2001). While the United States leaves most the protection of privacy to markets, "European democracies approach information privacy from the perspective of social protection" (Reidenberg 2001, p.731). Because in Europe the law is viewed as "the fundamental basis to pursue norms of social and citizen protection", the state is viewed as "the necessary player to frame the social community in which individuals develop and in which information practices must serve individual identity" (Reidenberg 2001, p.731).

The Data Protection Directive imposes obligations on the processors of personal data by requiring technical security and the notification of individuals whose data is collected, and also outlines circumstances under which data transfer may occur. Additionally, the Data Protection Directive gives individuals substantial rights to control the use of their personal data: (1) right to be informed that their personal data is being transferred (Article 12(a)); (2) the need to obtain "unambiguous" consent from the individual for the transfer of certain data (Article 7(a)); (3) the opportunity to make corrections to the data (Article 12); and (4) the right to object to the transfer of the data (Article 14).

Robinson et al. write that "data protection in Europe is not solely dependent on state-initiated regulation" (2009, p.8). The Data Protection Directive acknowledges and encourages self-regulatory approaches such as "sector specific codes of conduct at national and international levels, the conclusion of contracts implementing binding Model Clauses or Binding Corporate Rules to cover the exchange of personal data with a party outside of the European Union, and identity management to deal with challenges such as data ownership, data stewardship and data broking at a nonregulatory level" (N. Robinson et al. 2009, p.8).

9.7 United Kingdom

In the United Kingdom, online privacy is regulated by the Data Protection Act of 1998 (DPA), which essentially implements the Directive on Privacy and Electronic Communications (Stanaland et al. 2009, p.480). The DPA requires data controllers processing personal data to comply with data protection principles. Specifically, the data must be: (1) fairly and lawfully processed; (2) processed in accordance with individuals' rights; (3) accurate, adequate, relevant, and not excessive; (4) processed for limited purposes; (5); kept secure; and (6) not transferred to non-European Economic Area countries without adequate protection (Stanaland et al. 2009, p.480). The DPA is administered and implemented by the United Kingdom's Information Commissioner's Office (ICO). Stanaland et al. note that while the DPA establishes comprehensive requirements regarding general privacy protections, "there is no specific statute or directive specially dedicated to the cause of protecting children" (2009, p.480). The ICO has stated that "the fact that data protection law (at European and domestic level) does not draw any explicit distinction between data subjects who are adults and those who are children introduces an important extra dimension that must also be addressed" (ICO 2006, p.1).

On 2007, the ICO issued the Data Protection Good Practice Note (DPGPN) in an effort to assist individuals or businesses collecting personal data through websites. Pursuant to the DPGPN, "websites that collect information from children must have stronger safeguards in place to make sure any processing is fair" (ICO 2007, p.8). Since "children generally have a lower level of understanding than adults", notices explaining the way their information is used should be in a language "clear and appropriate to the age group the website is aimed at" and "should not exploit any lack of understanding" (ICO 2007, p.8). Websites should obtain parental consent before a child provides personal information, "unless it is reasonable to believe the child clearly understands what is involved and they are capable of making an informed decision". Explicit and verifiable parental consent is also needed for publishing children's personal data on the Internet or for disclosing or transferring such information to third parties (2007, p.9). Although the accepted methods for obtaining parental consent are not specified, the DPGPN advises that it will usually not be enough to ask children to confirm their parents have agreed by using a mouse click (2007, p.9). On the issue of verifiable parental consent, the Data Protection Note advised that it will usually not be considered adequate to request children to confirm that their parents agreed merely by the use of mouse click. More is required and business operators are advised to err on the side of the law and refrain from the proposed activity if obtaining verifiable parent consent entails a disproportionate effort on the part of the operator. Stanaland, Lwin & Leong note that although "these guidelines are a step toward more comprehensive protection of children online, they are suggestions rather than formal regulations, and compliance by website operators is voluntary" (Stanaland et al. 2009, p.480).

Some authors argue that in the United Kingdom, "soft law" codes have "overtaken the lack of intervention from the legislator" regarding children's privacy rights and data protection (Bartoli 2009, p.41). Like DPGPN, the Direct Marketing Association's Code of Practice for Commercial Communications to Children Online (DMA Code) requires verifiable parental consent before collection and/or disclosure of children's' personal data (Direct Marketing Association (DMA) 2002 Articles 5.1-5.2). A notice informing this requirement must be shown at the point where personal information is requested (Article 5.4). Article 5.4 further states that "this notice should be clear and prominent and written in language that will be easily understood by young children. It should include an explanation of the purposes for which data is being collected i.e. for marketing purposes and how that consent may be given to the Advertiser". The DMA Code, however, only protects the online privacy of children under 14. As a result, like COPPA, it leaves a considerable segment of our youth unprotected.

Finally, Prime Minister Gordon Brown recently announced the United Kingdom's "Click Clever Click Safe" strategy, a national plan that will "produce guidelines for government, industry and charities on how to protect children using the web" (Holden 2009). The new plan, which includes compulsory online safety lessons for children over 5, was created by the UK Council for Child Internet Safety, which is made up of over 140 organizations, including Google, Microsoft, and Bebo (Holden 2009).

10. Reputation

Reputation "plays an important role in society, and preserving private details of one's life is essential to it. We look to people's reputations to decide whether to make friends, go on a date, hire a new employee or undertake a prospective business deal" (Solove 2008, p.103). Our reputation is the collective or shared perception about us, which is "forged when people make judgments based upon the mosaic of information available about us" (Solove 2008, p.30). Since ancient times, one's reputation has been viewed as "indispensable to one's ability to engage in public life" (Solove & Schwartz 2009, p.173). Solove notes how "our reputation affects our ability to engage in basic activities in society" since:

> We depend upon others to engage in transactions with us, to employ us, to befriend us, and to listen to us. Without the cooperation of others in society, we often are unable to do what we want to do. Without the respect of others, our actions and accomplishments can lose their purpose and meaning. Without the appropriate reputation, our speech, though free, may fall on deaf ears. Our freedom, in short, depends in part upon how others in society judge us (2007, p.31).

Accordingly, "our reputation is an essential component to our freedom, for without the good opinion of our community, our freedom can become empty" (Solove 2007, p.30). Although reputation is an essential part of our freedom and identity, it is not solely our own creation. In every society, the way people talk about and evaluate the actions and traits of others has consequences for future interactions and reputations (Haidt 2001, pp.5-6; Solove 2007). As Haidt notes, an important subset of these evaluations are made with respect to virtues or goods that are expected from everyone in certain social categories (2001, p.6). "People who fail to embody these virtues, or whose actions betray a lack of respect for them, are subject to criticism, ostracism, or some other punishment" (Haidt 2001, p.6).

Children are social creatures whose judgments are strongly shaped by the judgments of those around them (Haidt 2001). Children's task in late childhood and adolescence is trying to fit into their peer groups, for it is among peers that alliances must be formed and prestige garnered (Harris 1995). Since much of peer socializing among young people goes on via social media, young people's conduct, both offline and online, is shaped by a general desire to be validated by their peers (boyd 2007; Christofides et al. 2009; Debatin et al. 2009; Valkenburg & Peter 2009). Boyd points out that "even though teens theoretically have the ability to behave differently online, the social hierarchies that regulate "coolness" offline are also present online" (2007, p.13). This can make activities that threaten reputation, such as bullying, distressing and upsetting to young people (Patchin & Hinduja 2006; Schrock & boyd 2008).

10.1 Concepts of Reputation

There have been no attempts to define reputation in common law (Post 1986; Yehudai 2008). Yehudai argues that "such an attempt would be futile, because reputation is a concept that keeps evolving and hence evades a single, static definition" (2008, p.819). Defamation law protects "an image of how people are tied together, or should be tied together, in a social setting" (Post 1986, p.693). As the concept of reputation evolves, so does the "nature of the reputation that the law of defamation seeks to protect" (Post 1986, p.693). Post identified three *concepts of reputation* that have had the most influence on the development of the common law of defamation, each of which corresponds to a different image of society. These concepts are reputation as *property*, as *honor*, and as *dignity* (Post 1986).

Reputation as property corresponds to "reputation in the marketplace" and "can be understood as a form of intangible property akin to goodwill" (Post 1986, p.693). Such a reputation can be earned through an "individual's efforts and labor", or "the exercise of a talent" (Post 1986, pp.693-694). The concept of reputation as property "presupposes that individuals are connected to each other through the institution of the market" because it is the market what "provides the mechanism by which the value of property is determined" (Post 1986, p.695). To injure someone's reputation in the marketplace without justification is to "unjustly destroy the results of an individual's labor. The resulting loss is "capable of pecuniary admeasurement" because the value of reputation is determined by the marketplace in exactly the same manner that the marketplace determines the cash value of any property loss" (Post 1986, p.694).

According to Post, the concept of reputation as property implies a "market society" with three distinctive features. First, because people are capable of creating their reputations, no matter what society's present estimation of an individual, he "always retains the capacity to work toward the production of a new reputation" (1986, pp.695-696). In a market society, individuals "possess personal identities that are distinct from and anterior to their social identities. Individuals are not constituted by the social regard with which they are apprehended by others" (1986, p.696). Second, "the worth of a person's reputation will vary with market conditions" (1986, p.696). Instead of an absolute, reputation is envisioned as a "smooth and continuous curve of potential value" that "will rise or fall depending upon an individual's productivity and upon fluctuations in market conditions" (1986, p.696). Third, all persons are equal, in the sense of that "no person has the right to a reputation other than that created by the evaluative processes of the market, and, conversely, every person enjoys an equal right to enter the market to attempt to achieve what reputation he can" (1986, p.696).

The concept of reputation as honor views an individual's reputation to be a "personal reflection of the status which society ascribes to his social position" (Post 1986, p.700). Instead of earning this honor through effort or labor, an individual "claims a right to it by virtue of the status with which society endows his social role" (Post 1986, p.700). In exchange for this benefit, "society expects him to aspire to "personify" the attributes and to make them part of his personal honor" (Post 1986, p.700). Contrary to reputation as property, reputation as honor considers individuals unequal because they occupy different social roles, which are hierarchically arranged (Post 1986). While reputation as property implies that individual identity is separate from reputation, in the sense that an individual can always construct a new reputation, the concept of honor presupposes that identity is "essentially, or at least importantly, linked to institutional roles" (Post 1986, p.701).

Contrary to reputation as property—which assumes that the value of reputation fluctuates according to individual effort and market conditions—reputation as honor is fixed into specific social roles and cannot be converted into a continuous medium of exchange (Post 1986, pp.700-701). Although reputation as honor cannot be individually created, it can be forfeited by "failing to fulfill the requirements of one's social position" (1986, p.701). Because honor is created by shared social perceptions that go beyond the behavior of particular individuals, honor is viewed as a public good and thus requires more than the protection individual interests (1986, p.702). Accordingly, if one's reputation is injured, so does the societal status structure, and thus to the social system. For example, in early common law, criticism of the king was viewed as injuring not only the monarch but also his government and possibly his relationship with his subjects (1986, p.702). Thus, "an assault on a person's reputation is considered an assault on the entire community, and as a consequence, the society's interest in protecting such reputation is viewed as equally important to the interest of the individual" (Yehudai 2008, p.820). An injury to a person's reputation "can scarcely be comprehended by pecuniary damages. Instead the essential objective of defamation law must be conceived as the restoration of honor" (Post 1986, p.703). For that reason, "reputation as honor is linked most closely to criminal libel, where the truth of the statement is immaterial and the plaintiff's redress is vindication" (Yehudai 2008, p.820).

Reputation as dignity refers to the "relationship between the private and public aspects of the self" (Post 1986, p.703). This third perspective presupposes that an individual's identity is the internalization "of the social connections by which he is embedded in and attached to a community. Dignity is therefore the respect of others and of self that arises from full membership in society" (Yehudai 2008, p.820). According to Post, implicit in this concept are two interests that defamation law must protect: (1) individuals' interest in maintaining social respect; and (2) society's interest in defining and maintaining the contours of its own social constitution (Post 1986, p.711).

The concept of reputation as dignity "creates two analytically and operationally distinct functions for defamation law: the rehabilitation of individual dignity and the maintenance of communal identity" (Post 1986, p.715). Both functions assume that reputation shapes individual identity in some way and, in this regard, the concepts of reputation as dignity and reputation as honor are similar (1986, p.715). However, "honor is concerned with attributes of personal identity that stem from the characteristics of particular social roles, whereas dignity is concerned with the aspects of personal identity that stem from membership in the general community" (1986, p.715). Contrary to reputation as property, dignity is not the result of individual achievement and its value cannot be measured in the marketplace nor its loss is capable of pecuniary admeasurements because it is "essential" and intrinsic in "every human being" (Post 1986, p.712).

Although these three concepts of reputation have been the most influential in the development of common law defamation, they are not the only possible concepts of reputation. Post notes, for example, how other cultures "have equated reputation with the judgment of history and immortal fame. Our own society recognizes the very special and unique form of reputation acquired by great leaders, heroes, or Nobel Prize winners. Their reputations are individually earned, and yet…their reputations are public treasures, not merely private possessions" (1986, p.720).

10.2 Reputation and the Internet

The Internet is prompting a large shift in what it means to built and manage one's identity (Palfrey & Gasser 2008, p.19). "Just as companies create corporate images that convey their core purpose and virtues, individuals project an online image through social networking sites, blogs, e-mail, photo and video sharing and other online activities" (Spanbauer 2006). The Internet is threatening people's ability to control their images and reputations (Palfrey & Gasser 2008; Solove 2007, 2008; Spanbauer 2006). As social reputation-shaping practices such as gossip and shaming migrate to the Internet, they are taking on new dimensions. Information that was once scattered, forgettable, and localized within small local groups is becoming widespread, permanent and searchable (Palfrey & Gasser 2008; Solove 2007, pp.4, 11).

10.3 Reputation and Youth Online

Many researchers believe that for young people, "the digital environment is simply an extension of the physical world" (Palfrey & Gasser 2008, p.19; boyd 2007). Palfrey & Gasser argue that digital natives "almost never distinguish between the online and offline versions of themselves. They establish and communicate their identities simultaneously in the physical and digital worlds" (2008, p.20). Because of this direct link between offline and online identities, teens are inclined to present the side of themselves that they believe will be well received by their peers (boyd 2007, p.13). Although youth's online activities largely replicate their existing practices of hanging out and communicating with friends, the characteristics of networked publics—public culture that is supported by online networks—"create new kinds of opportunities for youth to connect, communicate, and develop their public identities" (Ito et al. 2008, pp.10-11).

Boyd notes that social networking sites contain features that differentiate them from other types of computer-mediated communication: profiles, friends, and comments (2007). Social networking sites are "based around *Profiles*, a form of individual (or, less frequently, group) home page, which offers a description of each member" (boyd 2007, p.6). Besides text, images, and video created by each member, profiles also include a public list of the people that one identifies as *Friends* within the network, and *Comments* from other members. The importance of these practices, according to Boyd, is "that they take place in public: friends are publicly articulated, profiles are publicly viewed, and comments are publicly visible" (2007, p.7). Boyd argues that social networking sites are complicating the way in which people interact because they have four properties usually not present in face-to-face public life:

> *Persistence*: Unlike the ephemeral quality of speech in unmediated publics, networked communications are recorded for posterity. This enables asynchronous communication but it also extends the period of existence of any speech act.
>
> *Searchability*: Because expressions are recorded and identity is established through text, search and discovery tools help people find like minds. While people cannot currently acquire the geographical coordinates of any person in unmediated spaces, finding one's *digital body* online is just a matter of keystrokes.
>
> *Replicability*: Hearsay can be deflected as misinterpretation, but networked public expressions can be copied from one place to another verbatim such that there is no way to distinguish the "original" from the "copy."
>
> *Invisible audiences*: While we can visually detect most people who can overhear our speech in unmediated spaces, it is virtually impossible to ascertain all those who might run across our expressions in networked publics (2007, p.9).

The widespread publication of personal information over the Internet diminishes individual's ability to protect their reputation, thus making it more difficult to control one's identity and perceptions by others (Palfrey & Gasser 2008; Solove 2007, 2008). Palfrey & Gasser note:

> A sixteen-year-old girl's social identity, however, may be quite different from what it would have been in the agrarian or industrial ages. In the digital age, her social identity may be shaped by associations that are visible to onlookers at any moment through connections in social networks like MySpace, Facebook, Bebo, or studiVZ, or through links in her blog to the blogs of others. In turn, the actions of her friends, and their shifting reputations, can affect her identity and her reputation in ways that third parties can observe. Although she can change many aspects of her personal identity quickly and easily, she may not be able to change certain aspects of her social identity (2008, pp.19-20).

Solove considers that the explosion of Internet gossip is the main force behind individuals' loss of control over their reputations. According to Solove, Internet gossip is facilitating the use of public shaming as a tool for social control evocative of past shaming punishments such as branding, the pillory, and Hawthorne's scarlet letter, among others (2007, pp.90-92). In *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, Solove details modern "Internet shaming" such as websites like BitterWaitress.com—a site that allows servers to enter information about lousy tippers—and DontDateHimGirl.com, a site that allows women to denounce men who cheated on them (2007, pp.87-90).

Internet shaming creates a permanent record of a person's transgressions. Thanks to Google's cache and the Internet Archive's Wayback Machine, some of the online tracks people leave today—accurate or not—will remain fresh for decades to come (Solove 2007; Spanbauer 2006). Profiles on social networking sites won't always show up in a search engine query, but they will appear when members of those services track down the data subject (Spanbauer 2006). "In the past, oral gossip could tarnish a reputation, but it would fade from memories over time. People could move elsewhere and start anew" (Solove 2007, p.33). Being shamed in cyberspace, however, is capable of becoming a "digital scarlet letter" (2007, p.94).

10.4 Defamation

Society's "pervasive and strong interest in preventing and redressing attacks upon reputation" has given rise to the law of defamation (Post 1986, p.691). The law of defamation creates liability when a person makes a false statement about another that harms the person's reputation. To create liability for defamation there must be:

> a false and defamatory statement concerning another;
>
> an unprivileged publication to a third party;
>
> fault amounting at least to negligence on the part of the publisher; and
>
> either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication

(Restatement 2d of Torts, § 558). A statement is "defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him" (Restatement 2d of Torts, § 559). "One who publishes a defamatory statement of fact is not subject to liability for defamation if the statement is true" (Restatement 2d of Torts, § 581A). Thus, in order to be subject to liability for defamation, the published defamatory statement has to be false. The publication of a defamatory matter is "its communication intentionally or by a negligent act to one other than the person defamed"

(Restatement 2d of Torts, § 577). In addition, if a person "intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his control is subject to liability for its continued publication" (Restatement 2d of Torts, § 577). Moreover, "one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it", except "those who only deliver or transmit defamation published by a third person" (Restatement 2d of Torts, § 578).

Defamation law recognizes two torts: libel and slander. According to the Restatement:

> Libel consists of the publication of defamatory matter by written or printed words, by its embodiment in physical form or by any other form of communication that has the potentially harmful qualities characteristic of written or printed words.
>
> Slander consists of the publication of defamatory matter by spoken words, transitory gestures or by any form of communication other than those stated in Subsection (1).

(Restatement 2d of Torts, § 568). In determining whether a publication is a libel or slander, the following factors must be considered: "the area of dissemination, the deliberate and premeditated character of its publication and the persistence of the defamation" (Restatement 2d of Torts, § 568).

The First Amendment right to freedom of speech places some limits on defamation law. The United States Supreme Court held that the First Amendment precludes public officials and public figures—those who have achieved a general level of "notoriety" or who come to the "forefront of particular public controversies"—from receiving damages in defamation actions unless they could clearly and convincingly demonstrate that the communication at issue "was made with 'actual malice'—that is, with knowledge that it was false or with reckless disregard of whether it was false or not" (*Curtis Publishing Co. v. Butts*, 388 U.S. 130 (1967); *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974); *New York Times v. Sullivan*, 376 U.S. 254, 279-80 (1964)). While "famous people have to prove that the defendant intentionally told lies about them or simply didn't care whether rumors were true or not", private citizens need only show that the defendant was "negligent when he told lies, a much easier standard to establish" (Solove 2007, p.126).

Solove points out that "the Court crafted a compromise to balance the protection of free speech with the ability to seek redress for defamatory statements (2007, p.126). The Court has noted that although false statements are "not worthy of constitutional protection", they must be protected "if freedoms of expression are to have the 'breathing space' they need to survive" (*Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 340–41 (1974); *New York Times v. Sullivan*, 376 U.S. 254, 271–72 (1964)). However, it is also important to preserve the "individual's right to the protection of his own good name," which "reflects no more than our basic concept of the essential dignity and worth of every human being" (*Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 340–41 (1974)).

10.5 Objectionable Content and Online Intermediary Liability

The widespread publication of personal information over the Internet presents interesting problems for the application of defamation law (Solove & Schwartz 2009). As Solove & Schwartz note, defamatory or private information about individuals was traditionally communicated through news media (2009, p.175). While it was viable to sue these entities because they had the means to pay a judgment against them, this is not the case of the average person that posts a defamatory statement on the Internet (Solove & Schwartz 2009, p.175). Another difficulty is that defamatory statements are published anonymously. As a result, Internet service providers have been the focus of various defamation lawsuits. This prompted Congress to enact Section 230 of the Communications Decency Act of 1996 (CDA), which grants online services of all types, including blogs, social networking sites, forums, and listservs, broad immunity from certain types of legal liability streaming from content created by others.

Pursuant to Section 230, "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 U.S.C. § 230(c)(1)). Additionally, no provider or user of an interactive computer service shall be held liable on account of:

> any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1) (47 U.S.C. § 230(c)(2)).

Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions" (47 U.S.C. § 230(f)(2)).

Section 230 essentially creates a federal immunity to any cause of action that would make interactive computer service providers liable for information originating with a third-party user of the service (*Zeran v. American Online, Inc.*, 129 F.3d 327 (4th Cir. 1997)). Specifically, Section 230 precludes courts from entertaining claims that would place a service provider in a publisher's role. Accordingly, "lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are bared" (*Zeran v. American Online, Inc.*, 129 F.3d 327 (4th Cir. 1997)). In addition, where a state law contradicts the CDA, the state law is deemed preempted (*Zeran v. American Online, Inc.*, 129 F.3d 327 (4th Cir. 1997)). As a result of these policies, the remedies available to parties harmed by information published on the Internet are seriously limited (Mills 2008). Although the actual author of the harmful content may be liable, the prosecution of any claims against the author is likely to encounter substantial impediments to legal action since websites and Internet service providers are taking affirmative steps to preserve the anonymity of the author (Mills 2008).

Section 230 immunity was intended to protect "good Samaritan" Internet service providers from civil liability for blocking or screening objectionable online material (47 U.S.C. § 230(c)(2)). However, this section is being used to shield websites that traffic such content. According to Solove, "courts are interpreting Section 230 so broadly as to provide too much immunity, eliminating the incentive to foster a balance between speech and privacy. The way courts are using Section 230 exalts free speech to the detriment of privacy and reputation" (2007, p.159). Consequently, "a host of websites have arisen that encourage others to post gossip and rumors as well as to engage in online shaming" (2007, p.159). For example, the now-defunct JuicyCampus.com urged its users "C'mon. Give us the juice" and advertised itself as "the place to spill the juice about all the crazy stuff going on at your campus. It's totally anonymous, no registration, login, or email verification required" (McDonald, 2010). This website allowed people to anonymously post hateful, racist and defamatory speech without any oversight or removal. While Juicy Campus received a lot of attention and negative press, it was only one in a long list of websites that allow users to anonymously comment on their peers; other websites tackle teachers (RateMyTeachers.com), professors (RateMyProfessors.com), neighbors (RottenNeighbor.com) and law school students (AutoAdmit.com), among others.

Defamation is not the only area that has found refuge under the protection of Section 230 immunity. Courts have also extended Section 230 protection and thus found Internet service providers and websites immune from liability in cases where their servers were used to commit or facilitate the commission of crimes such as child pornography (*Jane Doe v. America Online*, 783 So. 2d 1010 (Fla. 2001)) and sexual assaults to minors (*Julie Doe v. Myspace.com*, 474 F. Supp. 2d 843 (W.D. Tex. 2007)). In *Julie Doe v. MySpace*, a 14-year-old girl created an account on MySpace in which she misrepresented her age as 18, gave out her telephone number, and arranged to meet a 19-year-old man who sexually assaulted her. After the man was arrested and charged with sexual assault, the girl's family decided to sue MySpace for making it too easy for minors to create profiles on their site and become vulnerable to online predators (*Julie Doe v. MySpace.com*, 474 F. Supp. 2d 848). Plaintiffs didn't based their case on MySpace's posting of third-party content, but rather on MySpace's failure to institute safety measures to protect minors (*Julie Doe v. MySpace.com*, 474 F. Supp. 2d 848). However, U.S. District Judge Sam Parks found that Section 230 reflects Congress's recognition that the potential for liability attendant to implementing safety features and policies creates a disincentive for interactive computer services to implement any safety features or policies at all (*Julie Doe v. MySpace.com*, 474 F. Supp. 2d 848). Because congressional policy in passing the CDA was to avoid chilling free speech rights, MySpace was not required to implement safety measures to protect minors from sexual predators and thus Plaintiffs' claims were barred by Section 230 (*Julie Doe v. MySpace.com*, 474 F. Supp. 2d 848).

Although the CDA has been smart not to chill free speech and innovation by placing too much liability on companies, the immunity is affecting children harmed online because it precludes their parents from even reaching the question of whether online intermediaries are in fact negligent (Palfrey & Gasser 2008). The law should not preclude parents from bringing a claim against websites for failing to protect the safety of their children, especially when the basis of the immunity is a "good Samaritan" statute like the CDA (Palfrey & Gasser 2008, p.106). As Palfrey and Gasser argue, there is no reason why a website like MySpace "should be protected from liability related to the safety of young people simply because its business operates online" (2008, p.107).

10.6 Proposed Solutions

Since the enactment of Section 230, a vibrant debate has ensued over how to strike the proper balance between the seemingly competing values of promoting free speech and compensating victims of objectionable speech or content. With Section 230 protecting online intermediaries from any liability associated with speech or content that some deem objectionable, legal scholars have proposed various alternatives to encourage more self-policing on online networks for objectionable content, including (1) leaving the question of negligence on the part of service providers to the tort regime; (2) adopting notice and takedown provisions modeled after the Digital Millennium Copyright Act; (3) completely repealing Section 230; thus, going back to the traditional publisher-distributor distinctions that govern traditional defamation suits; and (4) imposing liability on social networking sites that fail to adopt age verification requirements for all users.

Scholars argue that it is time to re-examine how far Section 230's immunity extends so that a claim is not barred at the courthouse door simply because the defendant is an interactive computer service. Palfrey believes that the question of negligence on the part of service providers should be left to the tort regime (Thierer 2009). Accordingly, if websites are "taking no steps to protect kids, or, worse, doing things affirmatively to encourage dangerous behavior, they would be found liable—on a sliding scale—for harm done to the child" (Thierer 2009, p. 2). Although such a proposal might chill speech and innovation to some degree, especially for many smaller websites and up-and-coming operators, as well as increase litigation, Palfrey considers this an acceptable price to pay in favor of greater safety for children online and offline (Thierer 2009, p. 2). Specifically, such a regime would have two important benefits. First, online service providers "would have greater incentive to take more ambitious steps, on an ongoing and dynamic basis, to protect kids from harm that comes to them as a result of their activities online. Second, we might see greater innovation, not less, in terms of technical safety measures to protect kids," since the market is driven by competition among online service providers (Thierer 2009, p. 2).

Authors have proposed a number of both legal and non-legal solutions to help individuals protect their reputations online. Solove argues that a notice and take-down system should substitute the broad immunity that websites currently enjoy because Section 230 "creates the wrong incentive, providing a broad immunity that can foster irresponsibility" (2007, p.159). However, Section 230 might be read in a different way: "to grant immunity only before the operator of a website is alerted that something posted there by another violates somebody's privacy or defames her. If the operator of a website becomes aware of the problematic material on the site, yet doesn't remove it, then the operator could be liable" (2007, p.154). This would foment the informal resolution of disputes, which is something the law should encourage and will often provide quick and inexpensive results (2007).

Solove's notice and take-down proposal has been criticized for different reasons. First, it doesn't provide the author an opportunity to request that the content be reposted (Heidlage 2008). Second, the proposal threatens bloggers' and Internet service providers' free-speech by "chilling their willingness to allow third-party comments or even to blog in the first place" (2008, pp.987-988). Finally, Solove's proposal "would reshape the nature and culture of blogs. Blogs are appealing in part because of their informal, off-the-cuff nature, which might be inhibited by a fear of litigation" (2008, p.988).

Other legal responses to the limitations on individuals' ability to protect their reputations from unwarranted damage on the Internet include expanding the tort of public disclosure of private facts in order to penalize bloggers who disclose the identities of the subjects of their posts (Solove 2007, 2008). Besides forcing people to act cautiously before revealing others' intimate details, this would also further interests in autonomy, democracy, and truth—the same interests that freedom of speech protects—by providing individuals with space in which to live and act (Solove 2007, pp.192-132). Others have proposed contract-based remedies as a substitute for the tort of public disclosure of private facts, arguing that this would protect free speech yet provide a remedy for certain intrusions (McClurg 2005). The basic idea is to find implied promises not to reveal certain intimate information. Similarly, Solove argues that the "law should more expansively recognize duties of confidentiality" (2007, p.176). The theory is to find "implicit promises of confidentiality when we share intimate information with others" (2007, p.176). The law already protects private information disclosed in privileged relationships—to doctors, lawyers and clergy. The confidentiality tort "could be strengthened to cover other relationships, such as spurned lovers, former friends or ex-spouses" (Solove 2008, p.103). Another important contribution the law can make is to "foster greater awareness of the difference between the offline and online spread of information" (Solove 2007, p.196).

It is possible that the law is not the best response to these problems (Palfrey & Gasser 2008; Solove 2007). Social norms, for example, have been considered to be "better and more effective constrains on behavior than law could ever be" (Meares 1996, p.594). Just like mainstream media developed norms to protect the privacy of rape victims and the family of politicians, the blogosphere should develop a code of ethics that persuades people to: (1) quickly delete offensive comments when asked; (2) ask permission before speaking about others' private lives or posting pictures of them online; (3) conceal the identity of those who do not consent to the divulgation of their private life; and (4) avoid Internet shaming (Solove 2007, pp.194-195).

Other solutions include the rise of services which helps people find and remove harmful information of themselves online (Solove 2007). ReputationDefender, for example, offers a service called MyChild, which according to the company's website:

> [S]cours the Internet for all references to your child or teen - by name, photography, screen name, or social network profiles - and packages it to you in an easy-to-understand report. Worried about bullies? Concerned that your teens' friends and peers are posting inappropriate materials online? MyChild searches every corner of the Internet for traces of your kids. If you want to help your teen manage their online reputation, but have felt powerless to do so, ReputationDefender is your answer! (2009)

It is also possible that the differences in the ways some adults and young people perceive privacy represents a persistent change; from this perspective, children and teenagers' sharing of "intimate secrets on the Web isn't the product of lack of maturity but instead is a manifestation of generational differences" (Solove 2007, p.197).

11.Supporting Online Youth Practice

11.1 Understanding Differing Conceptions of Privacy

Many studies of youth attitudes towards privacy equate “revealing personal information” with “privacy attitudes” (Turow & Nir 2000; Moscardelli & Divine 2007; Moscardelli & Liston-Heyes 2004; Moreno et al. 2007; Moreno et al. 2009; Steeves & Webster 2008; Wirth et al. 2007; Rosen et al. 2008; Lwin et al. 2008). However, qualitative and ethnographic studies repeatedly show that privacy and anonymity are not synonymous for many young people. Instead of viewing the public and the private as two strictly separate realms, children and teens show a more nuanced and granular understanding of information dissemination and control. For example, in their study of privacy on Facebook, West et. al. write:

> On the basis of our findings, interviewees did not appear to conceive of there being two distinct realms of the public and the private. Facebook was construed by some as part of the public or ‘semi-public’ sphere. Moreover, students in our sample conceptualized privacy in nuanced ways. Self-evidently, there are different groups of ‘friends’, some perhaps closer than others, some related some not, close older adult family members, older adults known socially, and employers. We could perhaps conceptualize these groups as real or perceived ‘delineations’ of an individual’s friends, family members and other contacts. These people share a common relationship to the individual on account of social, geographic, or historical factors with others in their group, but a different relationship to the individual from those people attributed to different groups. As a result, they engage in different behaviours with the individual and are party to different information about the individual (West et al. 2009, p.624)

Indeed, young people demonstrate an intense interest in controlling access to their personal information on a granular level (Livingstone 2008; Abril 2008; Tufekci 2008). In her ethnographic studies of teenagers, Livingstone found that “the question of what you show to others and what you keep private was often the liveliest part of the interviews, suggesting an intense interest in privacy” (2008, p.404).

Heather West, policy analyst at the Center for Democracy and Technology, writes in *Wired:*

> Rather than an all-or-nothing public or private paradigm, we expect to be able to choose levels of privacy and levels of exposure to the public. Most teens restrict access to their online profiles and do not think that sharing their information with a specific set of people means that the information is in the public domain. This allows them to both gain the benefits of sharing and communicating online, but also protecting their privacy and remain empowered in their choices about their

> own information. These expectations of granular control over information, both in the Pew studies on privacy controls and the more recent study on tailored content and advertising, seem to reflect the expectations of the Fair Information Practices (FIPs) that form the basis of most privacy law (2009).

What often befuddles adults is that the Internet is not seen by many young people as a *public* space. Online spaces like MySpace and Facebook are seen as *private social spaces* where young people can engage in personal talk, gossip, "hanging out", flirting, sharing secrets, and all the other social practices that they engage in with their peers offline (boyd 2008; Ito et al. 2008; Herring 2008; West et al. 2009; S. Jones et al. 2009; Steeves & Webster 2008; Christofides et al. 2009).

The extent to which online spaces are integrated into the social life of today's children and teenagers is often underestimated. Choosing to opt out or remain anonymous online can be socially disastrous for kids whose peer groups use IM, Facebook, MySpace, Xbox Live, YouTube and so forth. Friendships are established and solidified through the use of Internet communication technologies, and the provision of personal information is a way to establish trust between contemporaries (Steeves & Webster 2008; Christofides et al. 2009; Valkenburg & Peter 2009; Moinian 2006).

Protecting youth's privacy in a digital era, and everyone else's, will require reconciling people's desire to self-disclose information online with their simultaneous desire that this information be protected (Edwards & Brown 2009; Solove 2008). In order to achieve this, "society must develop a new and more nuanced understanding of public and private life—one that acknowledges that more personal information is going to be available yet also protects some choice over how that information is shared and distributed" (Solove 2008, p.104). Scholars have offered diverse solutions for protecting youth privacy in the digital era. However, as Palfrey and Gasser note, "there is no single, simple answer" and any solution is going to require the involvement of multiple actors, including young people, their parents and teachers, technology companies and policy makers (2008, p.69). Proposal for protecting privacy also must be balanced with other conflicting values, such as public safety and free speech (Mills 2008). True solutions not only will be complex, "they'll have to be global" (Palfrey & Gasser 2008, p.80).

11.2 Taking Responsibility

Adults have a responsibility to acknowledge their own roles in violating the privacy of children and adolescents. Although there is a lack of large-scale empirical research in this area, ethnographic and smaller-scale surveys suggest that surveillance in the home and in school are seen by children as significant privacy violations and may indeed threaten freedom of expression and a right to privacy. The popularization of monitoring and tracking gadgets such as GPS, baby monitors, webcams, CCTV, and so forth by schools and parents should be recognized and investigated in greater depth to determine the long-term effects on young people.

Second, the risks of revealing personal information online are often framed as parents, teachers, employers, administrators, and so forth finding young people's profiles and punishing them accordingly. However, there are currently no regulations to regulate law enforcement, university personnel, and the like from investigating young people's profiles, even when those profiles are set to "private" within a social network, for instance. The extent of these violations should be determined through future research, possibly as a basis for future legal recommendations regulating these types of investigations.

11.3 The Role of Education

There is certainly a role for greater privacy education for young people. However, this is frequently framed as a way to scare children away from social media, with an (unspoken) goal of preventing young people from sharing personal information:

> Adults are concerned about invasion of privacy, while teens freely give up personal information. This occurs because often teens are not aware of the public nature of the Internet (Barnes 2006).

As previously discussed, there is little evidence that teenagers do not care about privacy, and even less evidence that they do not understand how the Internet works. An approach to education that relies on exaggerating risks is ineffective and likely to do more harm than good; as Herring writes, there are negative impacts from these types of scare tactics:

> Youth know from their own experience and that of their friends that the Internet is not as dangerous as the popular media make it out to be. They may go ahead and do whatever they are not supposed to—chat with strangers, use Netspeak, swear, post provocative photos, visit pornographic websites—hoping to keep below adult radar. Such behavior constitutes an implicit rejection of adult "moral panics" about youth online (2008, p.80)

However, there is a need for greater media literacy so that young people can learn how to manipulate privacy settings on social media sites. Livingstone found that even groups of children who professed technical skill had a hard time with some of the complex settings on sites like Facebook or Bebo (2008). The sites themselves should provide comprehensive help information and make it clear to users what information is revealed or concealed at any one time.

Furthermore, any education that takes place needs to take into account the differences within groups of children and teenagers. Some of these differences are based around age cohorts. Yan suggests that children under 8 constitute a *vulnerable* population because they have limited experience with the Internet as well as limited understanding. He conceptualizes 9-10 year olds as in a *transitional* phase where more than Internet filters are needed to understand how to use the Internet safely. 11-12 year olds make up a more *emerging sophisticated* group who should be given the opportunity to use less restrictive filters (or unfiltered content) (Yan 2005).

Most importantly, understanding of youth norms *must* be comprehensive before heavy-handed proclamations and requirements are set in place (Ito et al. 2008, p.37)

11.4 Software Design

Technology companies can help protect youth privacy through technological design (Palfrey & Gasser 2008, p.70). Privacy in the digital era is not regulated by law or by informed user choice, but, as Lawrence Lessig famously noted, by *code* (Edwards & Brown 2009). Accordingly, technology companies should create more privacy-friendly interfaces and controls. Palfrey and Glasser suggest that companies that collect and store personal information “have an obligation to build secure systems, and they ought to be held accountable under the law if they don’t” (Palfrey & Gasser 2008, p.76).

11.5 Defaults

The power of defaults in software, and how they can be used and manipulated as policy tools, has been the subject of legal scholarship. As a matter of policy, defaults are good because they provide users with agency (Kesan & Shah 2006). According to Kesan & Shah, “users have a choice in the matter: they can go with the default option or choose another setting” (2006, p.596). Defaults also guide users by providing recommendations. Accordingly, defaults can influence users’ actions, shape norms and affect society. On the downside, defaults can disempower individuals because users, particularly in cyberspace, are prone to inertia and if users do not know about defaults, “they will assume that any alternative settings are impossible or unreasonable” (p. 596). Besides disempowering users who do not know or care that defaults can be changed, anti-privacy pro-data collection defaults are reinforcing inadequate privacy protection social and code-enforced norms (Edwards & Brown 2009). For example, the default code setting on Facebook allows anyone in a user’s network to see the personal details of any other user on that network. Consequently, those who join a network in good, though ignorant, faith are disclosing their personal data by default to every member of that network, some whom might be marketers, identity thieves, stalkers or worse (Edwards & Brown 2009).

One approach to determining defaults is the “would have wanted standard,” according to which “the default settings should be what the parties would have bargained for if the costs of negotiating were sufficiently low" (Kesan & Shah 2006). In theory, this standard ensures that the wishes of both parties are met in the design of defaults. However, users are likely to make unwise choices about their privacy because they are not fully informed, nor are they in a good position to make risk assessments balancing social advantage against privacy risks—especially the young and vulnerable (Edwards & Brown 2009).

Solove believes that the law should not force companies to set specific defaults, but the companies should be encouraged to think about the consequences that their architectural choices will have on the privacy of millions of people (Solove 2007, pp.201-203). On the contrary, Kesan & Shah identify three circumstances where policymakers may need to intervene and challenge the settings agreed to by users and developers to what the parties "would have NOT wanted." First, when users lack the knowledge and ability to change an important default setting, policymakers ought to use penalty defaults to shift the burden of the default to the developer. The government should implement a penalty default in order to protect users' information privacy, because it would force developers to notify and educate users before they have to share their personal information. Second, policymakers also need to intervene when default settings might cause harm to third parties. Finally, policymakers need to set defaults to comply with laws, regulations, or established legal principles. For example, COPPA sets a default rule that websites cannot collect information from children. Websites can switch from this default setting only if they have obtained parental consent (2006).

12.Conclusions

The prevailing discourse around youth and privacy assumes that young people don't care about their privacy because they post so much personal information online. The implication is that posting personal information online puts them at risk from marketers, pedophiles, future employers, and so on. Thus, policy and technical solutions are proposed that presume that young would not put personal information online if they understood the consequences.

However, our review of the literature suggests that young people care deeply about privacy, particularly with regard to parents and teachers viewing personal information. Young people are heavily monitored at home, at school, and in public by a variety of surveillance technologies. Children and teenagers want private spaces for socialization, exploration, and experimentation, away from adult eyes. Posting personal information online is a way for youth to express themselves, connect with peers, increase popularity, and bond with friends and members of peer groups. Subsequently, young people want to be able to restrict information provided online in a nuanced and granular way.

Much popular writing (and some research) discusses young people, online technologies, and privacy in ways that do not reflect the realities of most children and teenagers' lives. However, this provides rich opportunities for future research in this area. For instance, there are no studies of the impact of surveillance on young people-- at school, at home, or in public. Although we have cited several qualitative and ethnographic studies of young people's privacy practices and attitudes, more work in this area is needed to fully understand similarities and differences in this age group, particularly within age cohorts, across socioeconomic classes, between genders, and so forth. Finally, given that the frequently-cited comparative surveys of young people and adult privacy practices and attitudes are quite old, new research would be invaluable. We look forward to new directions in research in this area.

13. References

Abril, P.S., 2008. A (My) Space of One's Own: On Privacy and Online Social Networks. *Northwestern Journal of Technology and Intellectual Property*, 6(1), 73.

Acquisti, A. & Gross, R., 2006. Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Lecture notes in computer science*, 4258, 36–58.

Addington, L.A., 2009. Cops and Cameras: Public School Security as a Policy Response to Columbine. *American Behavioral Scientist*, 52(10), 1426-1446.

Aidman, A., 2000. Children's Online Privacy What you need to know about the Children's Online Privacy Protection Act. *Educational Leadership*, 58(2), 46–48.

Albrechtslund, A. & Dubbeld, L., 2005. The plays and arts of surveillance: Studying surveillance as entertainment. *Surveillance & Society*, 3(2/3), 216–221.

Andrejevic, M., 2007. *iSpy: Surveillance and power in the interactive era*, Lawrence, KS: University of Kansas Press.

Backett-Milburn, K. & Harden, J., 2004. How children and their families construct and negotiate risk, safety and danger. *Childhood*, 11(4), 429.

Barnes, B., 2009. Bigger Screen for a High-Pitched Whine. *The New York Times*. Available at: http://www.nytimes.com/2009/12/08/movies/08fred.html?_r=2 [Accessed December 17, 2009].

Barnes, S., 2006. A Privacy Paradox: Social Networking in the United States. *First Monday*, 11(9). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394 [Accessed August 25, 2009].

Bartoli, E., 2009. Children's Data Protection vs. Marketing Companies. *International Review of Law, Computers & Technology*, 23(1-2), 35-45.

Bechar-Israeli, H., 1996. FROM <Bonehead> TO <cLoNehEAd>: *Journal of Computer-Mediated Communication*, 1(2). Available at: http://jcmc.indiana.edu/vol1/issue2/bechar.html [Accessed January 10, 2009].

Bellman, S. et al., 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20, 313-324.

Bennett, C.J. & Raab, C.D., 2006. *The governance of privacy*, Cambridge, MA: MIT Press.

Berson, I.R. & Berson, M.J., 2006. Children and Their Digital Dossiers. *International Journal of Social Education*, 21(1), 135-147.

Birkland, T.A. & Lawrence, R.G., 2009. Media Framing and Policy Change After Columbine. *American Behavioral Scientist*, 52(10), 1405-1425.

Boneva, B.S. & Quinn, A., 2006. Teenage communication in the instant messaging era. In R. E. Kraut, S. Kiesler, & I. Shklovski, eds. *Computers, phones, and the Internet: Domesticating information technology*. Oxford, England: Oxford University Press, pp. 201–218.

Bovill, M. & Livingstone, S., 2001. Bedroom culture and the privatization of media use. *Children and their changing media environment: A European comparative study*, 179–200.

boyd, D., 2008. *Taken out of context: American teen sociality in networked publics*. University of California, Berkeley. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1344756.

boyd, D., 2007. Why Youth (Heart) Social Network Sites: The Role of Networked Publics. In D. Buckingham, ed. *Youth, Identity and Digital Media*. Cambridge, MA: MIT Press, pp. 119–142.

boyd, D. & Ellison, N., 2007. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1). Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

Cai, X. & Gantz, W., 2000. Online privacy issues associated with web sites for children. , 44(2), 197-214.

Calabrese, C., 2009. Technology Changes Things. Latest Example: Student Records. *ACLU Blog of Rights: Technology and Liberty*. Available at: http://www.aclu.org/blog/technology-and-liberty/technology-changes-things-latest-example-student-records [Accessed December 16, 2009].

Campbell, R., 2006. Teenage Girls and Cellular Phones: Discourses of Independence, Safety and Rebellion'. *Journal of Youth Studies*, 9(2), 195–212.

Canadian Marketing Association, 2009. Code of Ethics and Standards of Practice. Available at: http://www.the-cma.org/?WCE=C=47|K=225849#11 [Accessed December 22, 2009].

Caverlee, J. & Webb, S., 2008. A large-scale study of MySpace: Observations and implications for online social networks. In *2nd International Conference on Weblogs and Social Media (AAAI)*.

Christofides, E., Muise, A. & Desmarais, S., 2009. Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, 12(3), 341–345.

Ciocchetti, C.A., 2007. E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. *American Business Law Journal*, 44(1), 55–126.

Cullen, R. & Reilly, P., 2007. Information Privacy and Trust in Government: a citizen-based perspective from New Zealand. In Hawaii, pp. 109–109.

De Souza, Z. & Dick, G.N., 2009. Disclosure of information by children in social networking—Not just a case of "you show me yours and I'll show you mine". *International Journal of Information Management*, 29(4), 255-261.

Debatin, B. et al., 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108.

Devitt, K. & Roker, D., 2009. The Role of Mobile Phones in Family Communication. *Children & Society*, 23(3), 189-202.

Direct Marketing Association (DMA), 2002. *The DMA Code of Practice for Commercial Communications to Children On Line*, Available at: myschoollunch.co.uk/Telford/files/general/DMA_Code.pdf.

Directive 2002/58/EC of the European Parliament, 2002. Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. *Official Journal of the European Communities*, 201, 37-47.

Directive 95/46/ec of the European Parliament, 1995. Directive 95/46/ec of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official*

Journal of the European Communities, 281, 31-50.

Dwyer, C., Hiltz, S.R. & Passerini, K., 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of AMCIS*.

Eastin, M.S., Greenberg, B.S. & Hofschire, L., 2006. Parenting the Internet. *Journal of Communication*, 56(3), 486-504.

Edwards, L. & Brown, I., 2009. Data Control and Social Networking: Irreconcilable Ideas? In A. Matwyshyn, ed. *Harboring Data: Information Security, Law and the Corporation*. Stanford, CA: Stanford University Press, pp. 202-227.

Ellison, N., Heino, R. & Gibbs, J., 2006. Managing impressions online: Self-presentation processes in the online dating environment. *Journal of Computer-Mediated Communication*, 11(2), 415.

Ellison, N., Steinfield, C. & Lampe, C., 2007. The benefits of Facebook" friends:" social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143.

Elsley, S., 2004. Children's experience of public space. *Children & Society*, 18(2), 155-164.

European Convention on Human Rights, 1950. *European Convention on Human Rights: The Convention for the Protection of Human Rights and Fundamental Freedoms*,

Federal Trade Commission, 2007. *Implementing the Children's Online Privacy Protection Act: A Report to Congress*, Washington, DC: Federal Trade Commission. Available at: http://www.ftc.gov/ reports/coppa/07COPPA_Reportto_Congress.pdf.

Federal Trade Commission, 1998. *Privacy Online: A Report to Congress*, Washington, DC: Federal Trade Commission. Available at: http://ftc.gov/reports/privacy3/toc.shtm.

Fogel, J. & Nehmad, E., 2009. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153–160.

Fotel, T. & Thomsen, T.U., 2004. The Surveillance of Children's Mobility. *Surveillance and Society*, 1(4), 535-554.

Friedman, B., Khan Jr, P.H. & Howe, D., 2000. Trust online. *Communications of the ACM*, 43(12), 34-40.

Fukuyama, F., 1996. Trust still counts in a virtual world. *Forbes ASAP Supplement*, 1337051, 33-34.

Gambrell, E., 2009. Teen Fashion Bloggers. *Teen Vogue*. Available at: http://www.teenvogue.com/industry/2009/02/teen-fashion-bloggers?printable=true [Accessed December 17, 2009].

Gibbs, J.L., Ellison, N. & Heino, R.D., 2006. Self-presentation in online personals: The role of anticipated future interaction, self-disclosure, and perceived success in Internet dating. *Communication Research*, 33(2), 152.

Giffen, M., 2008. Online Privacy. *Current Health*, 34(7), 8-11.

Giroux, H., 2003. Racial injustice and disposable youth in the age of zero tolerance. *International Journal of Qualitative Studies in Education*, 16(4), 553–565.

Gottschalk, L., 2006. Internet filters in public libraries: do they belong? *Library Student Journal*. Available at: http://www.librarystudentjournal.org/index.php/lsj/article/viewArticle/25/17 [Accessed December 16, 2009].

Govani, T. & Pashley, H., 2007. *Student awareness of the privacy implications when using Facebook*, Carnegie Mellon University. Available at: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf.

Grant, I. & O'Donohoe, S., 2007. Why young consumers are not open to mobile marketing communication. *International Journal of Advertising*, 26(2), 223.

Grant, I.C., 2006. Online Privacy: An Issue for Adolescents. In *Proceedings of the Child and Teen Consumption Conference*. Copenhagen.

Grant, I.C., 2005. Young Peoples' Relationships with Online Marketing Practices: An Intrusion Too Far? *Journal of Marketing Management*, 21(5), 607–623.

Grinter, R.E. & Palen, L., 2002. Instant messaging in teen life. In *Proceedings of the 2002 ACM conference on Computer supported cooperative work*. pp. 21–30.

Gross, E.F., 2004. Adolescent Internet use: What we expect, what teens report. *Journal of Applied Developmental Psychology*, 25(6), 633–649.

Gross, R. & Acquisti, A., 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. New York: ACM Press, pp. 71-80.

Haidt, J., 2001. The emotional dog and its rational tail: A social intuitionist approach to moral judgment. *Psychological Review*, 108(4), 814–834.

Harris, J.R., 1995. Where is the child's environment? A group socialization theory of development. *Psychological Review*, 102(3), 458–489.

Heidlage, B.F., 2008. Limiting the Scarlet @: Daniel J. Solove's The Future of Reputation. *New York University Law Review*, 83, 982–1979.

Heins, M., Cho, C. & Feldman, A., 2006. *Internet Filters: A Public Policy Report*, New York: Brennan Center for Justice at NYU School of Law.

Henderson, S. & Gilding, M., 2004. 'I've Never Clicked this Much with Anyone in My Life': Trust and Hyperpersonal Communication in Online Friendships. *New Media & Society*, 6(4), 487.

Henke, L.L., 2002. After the Internet: A Third-Year Follow Up and Comparative Analysis of Children's Perceptions and Use of the Internet. *Proceedings of the Academy of Marketing Studies*, 7(25).

Henke, L.L., 1999. Children, advertising, and the Internet: An exploratory study. In D. Schumann & E. Thorson, eds. *Advertising and the World Wide Web*. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 73–80.

Herring, S.C., 2008. Questioning the generational divide: Technological exoticism and adult construction of online youth identity. In D. Buckingham, ed. *Youth, Identity, and Digital Media*. Cambridge, MA: MIT Press, pp. 71-94.

Hiller, J. et al., 2008. Pocket Protection. *American Business Law Journal*, 45(3), 417–775.

Hinduja, S. & Patchin, J.W., 2008. Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence*, 31(1), 125–146.

Holden, M., 2009. UK makes online safety lessons for kids compulsory - Yahoo! News. *Yahoo! News*. Available at: http://news.yahoo.com/s/nm/20091208/wr_nm/us_britain_Internet [Accessed December 21, 2009].

Hope, A., 2009. CCTV, school surveillance and social control. *British Educational Research Journal*, 35(6), 891.

Hope, A., 2005. Panopticism, play and the resistance of surveillance: case studies of the observation of student Internet use in UK - schools. *British Journal of Sociology of Education*, 26(3), 359.

Hope, A., 2007. Risk Taking, Boundary Performance and Intentional School Internet "Misuse". *Discourse: Studies in the Cultural Politics of Education*, 28(1), 87.

Howe, N. & Strauss, W., 2000. *Millennials rising*, New York: Random House, Inc.

Huffaker, D., 2006. Teen blogs exposed: The private lives of teens made public. In *Proceedings of the American Association for the Advancement of Science Conference*. St. Louis, MO.

Huffaker, D.A. & Calvert, S.L., 2005. Gender, identity, and language use in teenage blogs. *Journal of Computer-Mediated Communication*, 10(2), 1.

Information Commissioner's Office (ICO), 2007. Data Protection Good Practice Note: Collecting Personal Information Using Websites. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf.

Information Commissioner's Office (ICO), 2006. Protecting Children's Personal Information: ICO Issues Paper. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/issues_paper_protecting_childrens_personal_information.pdf.

Ito, M. et al., 2008. Living and Learning with New Media: Summary of Findings from the Digital Youth Project. *The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning*, 52.

Joinson, A.N., 2008. Looking at, looking up or keeping up with people?: motives and use of facebook. In *CHI 2008 Proceedings - Online Social Networks*. Florence, Italy.

Jones, H. & Soltren, J.H., 2005. Facebook: Threats to privacy. *Project MAC: MIT Project on Mathematics and Computing*.

Jones, S. & Fox, S., 2009. *Generations online in 2009*, Washington, DC: Pew Internet &

American Life Project.

Jones, S. et al., 2009. Everyday life, online: U.S. college students' use of the Internet. *First Monday*, 14(10). Available at: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2649/2301 [Accessed October 13, 2009].

Kesan, J.P. & Shah, R.C., 2006. Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics. *Notre Dame Law Review*, 82(2), 583–634.

Kornblum, J., 2007. Online privacy? For young people, that's old-school. *USA Today*. Available at: http://www.usatoday.com/tech/webguide/Internetlife/2007-10-22-online-privacy_N.htm [Accessed October 13, 2009].

Kumaraguru, P. & Cranor, L.F., 2005. Privacy indexes: A survey of Westin's studies. *Institute for Software Research International*.

Lampe, C., Ellison, N. & Steinfield, C., 2008. Changes in use and perception of facebook. In *Proceedings of the ACM 2008 conference on Computer supported cooperative work*. pp. 721–730.

Lenhart, A., 2009. *Teens and Mobile Phones Over the Past Five Years: Pew Internet Looks Back*, Washington, DC: Pew Internet & American Life Project.

Lenhart, A. & Madden, M., 2007. *Teens, Privacy and Online Social Networks*, Washington, DC: Pew Internet & American Life Project. Available at: http://www.pewInternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx [Accessed August 25, 2009].

Lenhart, A. et al., 2007. *Teens and social media*, Washington, DC: Pew Internet & American Life Project.

Lindström, M., 2001. *Clicks, bricks & brands*, Victoria, Australia: Kogan Page Publishers.

Littman, M., 2000. How Marketers Track Underage Consumers. *Marketing News*, 8.

Liu, H., 2007. Social network profiles as taste performances. *Journal of Computer-Mediated Communication*, 13(1), 252.

Livingstone, S., 2006. Children's Privacy Online: Experimenting with boundaries within and beyond the family. In R. Kraut, M. Brynin, & Kiesler, Sara, eds. *Computers, Phones, and the Internet: Domesticating Information Technology*. Oxford, England: Oxford University Press, pp. 128–44.

Livingstone, S., 2005. Mediating the public/private boundary at home. *Journal of Media Practice*, 6(1), 11p-151.

Livingstone, S., 2007. Strategies of parental regulation in the media-rich home. *Computers in Human Behavior*, 23(3), 920-941.

Livingstone, S., 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media Society*, 10(3), 393-411.

Lwin, M.O., Stanaland, A.J. & Miyazaki, A.D., 2008. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing*, 84(2), 205-217.

Lyon, D., 2001. *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press.

Martin, C., 1998. Mailing Lists, Mailboxes, and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem. *Houston Law Review*, 35, 801.

Marwick, A., 2009. There's no hiding on Facebook. *The Guardian*. Available at: http://www.guardian.co.uk/commentisfree/cifamerica/2009/oct/05/facebook-privacy-beacon-lawsuit [Accessed December 14, 2009].

Marwick, A. & boyd, D., To See and Be Seen: Celebrity Practice on Twitter. *In Review*.

McDonald, S., 2010. Defamation in the Internet Age: Why Roommates.com isn't enough to change the rules for anonymous gossip websites. *Florida Law Review* 62, 259.

McClurg, A.J., 2005. Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality. *University of Cincinnati Law Review*, 74, 887.

McLean, R. & Griffiths, M., 2009. Washing the Dirty Linen: Exploring the Increasing Publication of Private Lives through New Social Media. In Milwaukee.

Meares, T.L., 1996. It's a Question of Connections. *Val. UL Rev.*, 31, 579.

Mesch, G.S., 2009. Parental Mediation, Online Activities, and Cyberbullying. *CyberPsychology & Behavior*, 12(4), 387-393.

Milberg, S.J. et al., 1995. Values, personal information privacy, and regulatory approaches. *Communications of the ACM*, 38, 65-74.

Mills, J.L., 2008. *Privacy: the lost right*, Oxford, England: Oxford University Press.

Moinian, F., 2006. The Construction of Identity on the Internet: Oops! I've left my diary open to the whole world! *Childhood*, 13(1), 49.

Monahan, T., 2006. *Surveillance and security*, CRC Press.

Montgomery, K. & Pasnik, S., 1996. *Web of deception: Threats to children from online marketing*, Washington, DC: Center for Media Education.

Moreno, M.A., Parks, M. & Richardson, L.P., 2007. What Are Adolescents Showing the World About Their Health Risk Behaviors on MySpace? *Medscape General Medicine*, 9(4), 9.

Moreno, M.A. et al., 2009. Reducing at-risk adolescents' display of risk behavior on a social networking Web site: a randomized controlled pilot intervention trial. *Archives of Pediatrics & Adolescent Medicine*, 163(1), 35.

Moscardelli, D.M. & Divine, R., 2007. Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal*, 35(3), 232-252.

Moscardelli, D.M. & Liston-Heyes, C., 2004. Teens Surfing The Net: How Do They Learn To Protect Their Privacy? *Journal of Business and Economics Research*, 2(9), 43-56.

Nelson, M.K., 2008. Watching Children: Describing the Use of Baby Monitors on Epinions.com. *Journal of Family Issues*, 29(4), 516-538.

Nemati, H., Tao, W. & Gold, J., 2003. Understanding Tradeoffs: The Link Between Knowledge and Privacy Concerns. In *Proceedings of the 34th Annual Meeting of the Decision Sciences Institute Meeting*. Washington, DC. Available at: [Accessed December 21, 2009].

Nissenbaum, H., 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.*, Palo Alto, California, USA: Stanford University Press.

Nussbaum, E., 2007. Kids, the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll. *New York Magazine*. Available at: http://nymag.com/news/features/27341/ [Accessed October 13, 2009].

Organization for Economic Cooperation and Development (OECD), 1981. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: Organisation for Economic Co-operation and Development; Washington, DC: OECD Publications and Information Center.

Pain, R. et al., 2005. 'So Long as I Take my Mobile': Mobile Phones, Urban Life and Geographies of Young People's Safety. *International Journal of Urban and Regional Research*, 29(4), 814-830.

Palfrey, J., 2008. The Public and the Private at the United States Border with Cyberspace. Mississippi Law Journal 78: 241-294.

Palfrey, J. & Gasser, U., 2008. *Born Digital: Understanding the First Generation of Digital Natives*, New York: Basic Books.

Palfrey, J., Sacco, D. & boyd, D., 2008. *Enhancing Child Safety and Online Technologies: Research Advisory Board Report for the Internet Safety Technical Task Force*, Cambridge, MA: The Berkman Center for Internet and Society at Harvard University.

Patchin, J.W. & Hinduja, S., 2006. Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, 4(2), 148.

Patil, S. & Kobsa, A., 2005. Uncovering privacy attitudes and practices in instant messaging. In *Proceedings of the 2005 international ACM SIGGROUP conference on Supporting group work*. pp. 109–112.

Post, R.C., 1986. Social Foundations of Defamation Law: Reputation and the Constitution, The. *California Law Review*, 74, 691.

Public Interest Advocacy Center (PIAC), 2008. All in the Data Family: Children's Privacy Online. Available at: http://www.piac.ca/files/children_final_small_fixed.pdf.

Raman, P. & Pashupati, T.K., 2005. Online privacy: the impact of self perceived technological competence. In *Contemporary Research in E-Marketing*. Hershey, PA: Idea Group Inc., pp. 200-225.

Read, B., 2006. Think Before You Share. *The Chronicle of Higher Education*, 52(20), A38-A41.

Reidenberg, J., 2001. E-Commerce and Trans-Atlantic Privacy. *Houston Law Review*, 38, 717.

Reidenberg, J. & Debelak, J., 2009. *Children's Educational Records and Privacy*, Fordham University, New York: Center on Law and Information Policy.

ReputationDefender, 2009. Protect my child's online identity : My Child : Reputation Defender. *Reputation Defender.com*. Available at: http://www.reputationdefender.com/mychild [Accessed December 21, 2009].

Robinson, N. et al., 2009. *Review of EU Data Protection Directive: Inception Report*, RAND Europe: Information Commissioner's Office. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf.

Rosen, L.D., Cheever, N.A. & Carrier, L.M., 2008. The association of parenting style and child age with parental limit setting and adolescent MySpace behavior. *Journal of Applied Developmental Psychology*, 29(6), 459-471.

Rotenberg, M., 2001. Fair Information Practices and the Architecture of Privacy:(What Larry Doesn't Get). *Stanford Technology Law Review*, 2001, 1–4.

Rousseau, D. et al., 1998. Not so different after all: a cross-descipline view of trust. *Academy of Management Review*, 23(3), 404, 393.

Schrock, A. & boyd, D., 2008. *Online Threats to Youth: Solicitation, Harassment, and Problematic Content.*, Cambridge, MA: Berkman Center for Internet and Society at Harvard University. Available at: http://cyber.law.harvard.edu/pubrelease/isttf/.

Senft, T., 2008. *Camgirls: Celebrity and Authenticity in the Age of Social Networks*, New York: Peter Lang.

Sheehan, K.B. & Hoy, M.G., 2000. Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing*, 19(1), 62–73.

Sheehan, K.B. & Hoy, M.G., 1999. Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising*, 28(3), 37–51.

Solove, D. J., 2002. Digital Dossiers and the Dissipation of Fourth Amendment Privacy. Southern California Law Review 75:1083.

Solove, D.J., 2002. Conceptualizing Privacy. *California Law Review*, 90, 1087.

Solove, D.J., 2005. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477.

Solove, D.J., 2004. *The digital person: Technology and privacy in the information age*, New York: NYU Press.

Solove, D.J., 2008. The end of privacy? *Scientific American*, 299(3), 100.

Solove, D.J., 2007. *The future of reputation: gossip, rumor, and privacy on the Internet*, Yale University Press.

Solove, D.J., 2008. *Understanding privacy*, Harvard University Press.

Solove, D.J., Rotenberg, M. & Schwartz, P.M., 2006. *Information privacy law*, Aspen Publishers.

Solove, D.J. & Schwartz, P.M., 2009. *Information Privacy Law, 3rd Edition*, Aspen Publishers.

Spanbauer, S., 2006. Safeguard your reputation while socially networking. *PC World*, 24(10), 152-154.

Stanaland, A.J., Lwin, M.O. & Leong, S., 2009. Providing Parents with Online Privacy Information: Approaches in the US and the UK. *Journal of Consumer Affairs*, 43(3), 474-494.

Steeves, V. & Webster, C., 2008. Closing the barn door: the effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society*, 28(1), 4-19.

Steeves, V. & Wing, C., 2005. Young Canadians in a wired world phase II: Trends and recommendations. *Media Awareness Network. Ottawa, Ontario*.

Subrahmanyam, K. & Greenfield, P., 2008. Online communication and adolescent relationships. *Children and Electronic Media*, 18(1), 119–146.

Subrahmanyam, K., Greenfield, P.M. & Tynes, B., 2004. Constructing sexuality and identity in an online teen chat room. *Journal of Applied Developmental Psychology*, 25(6), 651–666.

Taylor, T.L., 2006. Does WoW change everything?: How a PvP server, multinational player base, and surveillance mod scene caused me pause. *Games and Culture*, 1(4), 318.

The New York Times, 2009. Twitter Tapping. *The New York Times*. Available at: http://www.nytimes.com/2009/12/13/opinion/13sun2.html [Accessed December 14, 2009].

Thierer, A., 2009. Dialogue: the future of online obscenity and social networks. *Ars Technica.* Available at http://arstechnica.com/tech-policy/news/2009/03/a-friendly-exchange-about-the-future-of-online-liability.ars/ [Accessed January 26, 2010].

Thomas, A., 2007. Blurring and Breaking through the Boundaries of Narrative, Literacy, and Identity in Adolescent Fan Fiction. In M. Knobel & C. Lankshear, eds. *A New Literacies Sampler*. New Literacies & Digital Epistemologies. New York: Peter Lang, pp. 137-166.

Tufekci, Z., 2008. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20.

Turow, J., 2001. Family boundaries, commercialism, and the Internet: A framework for research. *Journal of Applied Developmental Psychology*, 22(1), 73–86.

Turow, J., 2006. *Niche envy: Marketing discrimination in the digital age*, The MIT Press.

Turow, J. & Nir, L., 2000. The Internet and the family 2000: The view from parents, the view from kids. *Philadelphia, PA: Annenberg Public Policy Center, University of Pennsylvania. Retrieved October*, 20, 2005.

U.S. Children's Online Privacy Protection Act, 1998. *U.S. Children's Online Privacy Protection Act of 1998 (COPPA).*,

United States Department of Health, Education and Welfare, 1973. *Code of Fair Information Practices*, Washington, DC. Available at: http://epic.org/privacy/hew1973report/.

Valentine, G., 2004. *Public space and the culture of childhood*, Farnham, UK: Ashgate Publishing, Ltd.

Valkenburg, P.M. & Peter, J., 2008. Adolescents'identity experiments on the Internet: Consequences for social competence and self-concept unity. *Communication Research*, 35(2), 208.

Valkenburg, P.M. & Peter, J., 2009. The Effects of Instant Messaging on the Quality of Adolescents' Existing Friendships: A Longitudinal Study. *Journal of Communication*, 59(1), 79-97.

Van Rompaey, V., Roe, K. & Struys, K., 2002. Childrens Influence on Internet Access at Home: Adoption and use in the family context. *Information, Communication and Society*, 5(2), 189-206.

Veigas, F.B., 2005. Bloggers' expectations of privacy and accountability: An Initial Survey. *Journal of Computer-Mediated Communication*, 10(3). Available at: http://jcmc.indiana.edu/vol10/issue3/viegas.html.

Wang, R., Bianchi, S.M. & Raley, S.B., 2005. Teenagers' Internet Use and Family Rules: A Research Note. *Journal of Marriage and Family*, 67(5), 1249-1258.

Warren, S.D. & Brandeis, L.D., 1890. Right to Privacy. *Harvard Law Review*, 4, 193.

West, A., Lewis, J. & Currie, P., 2009. Students' Facebook ‘friends’: public and private spheres. *Journal of Youth Studies*, 12(6), 615–627.

West, H., 2009. Is Online Privacy a Generational Issue? *GeekDad, Wired.com*. Available at: http://www.wired.com/geekdad/2009/10/is-online-privacy-a-generational-issue/ [Accessed November 16, 2009].

Westin, A.F., 1967. *Privacy and Freedom*, New York: Atheneum Press.

Westin, A.F., 2003. Social and political dimensions of privacy. *Contemporary Perspectives on Privacy: Social, Psychological, Political*, 59(2), 431–453.

Williams, M. et al., 2005. Children and emerging wireless technologies: Investigating the potential for spatial practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. pp. 02–07.

Wirth, C.B. et al., 2007. *Promoting Teenage Online Safety with an i-Safety Intervention: Enhancing Self-efficacy and Protective Behaviors*, Citeseer.

Wolak, J., Finkelhor, D. & Mitchell, K.J., 2008. Is Talking Online to Unknown People Always Risky? Distinguishing Online Interaction Styles in a National Sample of Youth Internet Users. *CyberPsychology & Behavior*, 11(3), 340-343.

Wolak, J., Finkelhor, D., Mitchell, K.J. & Ybarra, M.L., 2008. Online"Predators"and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. *American Psychologist*, 63(2), 111.

Wong, R., 2005. Privacy: Charting its Developments and Prospects. In M. Klang & A. Murray, eds. *Human Rights in the Digital Age*. London: The GlassHouse Press, pp. 147-162.

Working Group of Canadian Privacy Commissioners and Child and Youth Advocates (Canadian Working Group), 2009. *There Ought to be a Law: Protecting Children's Online Privacy in the 21st Century.*, Available at: http://www.gnb.ca/0073/PDF/Children'sOnlinePrivacy-e.pdf.

Xie, E., Teo, H. & Wan, W., 2006. Volunteering personal information on the Internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing Letters*, 17(1), 61-74.

Yan, Z., 2005. Age differences in children's understanding of the complexity of the Internet. *Journal of Applied Developmental Psychology*, 26(4), 385–396.

Yan, Z., 2006. What influences children's and adolescents' understanding of the complexity of the Internet? *Developmental psychology*, 42(3), 418.

Yehudai, C., 2008. Informational Blackmail: Survived by Technicality. *Marquette Law Review*, 92, 779.

Youn, S., 2009. Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, 43(3), 389-418.

Youn, S., 2008. Parental Influence and Teens' Attitude toward Online Privacy Protection. *Journal of Consumer Affairs*, 42(3), 362–388.

Youn, S., 2005. Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86.

Youn, S. & Hall, K., 2008. Gender and Online Privacy among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors. *CyberPsychology & Behavior*, 11(6), 763–765.

Zhao, S., Grasmuck, S. & Martin, J., 2008. Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior*, 24(5), 1816-1836.