UNDERSTANDING SECURITY WITHIN SOCIAL MEDIA IN RELATION TO ADOLESCENT USE

A THESIS

Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Information Assurance

Department of Information Assurance
School of Computer & Information Sciences
Regis University

By

Dale Hufford

Originally Submitted: May 12, 2015
Revised and Updated Edition: 2026

Thesis Advisor: Jennifer Kurtz

Committee Member: Shari Plantz-Masters

Abstract

With the rapid evolution of social media, platforms such as Facebook—now operating under the parent company Meta—have grown to encompass billions of users globally. This study examines social networking as a whole, with particular focus on how platforms manage privacy for minors, how parents perceive existing security controls, and whether those perceptions align with reality. Studies show that an individual's attitude toward using privacy controls is directly influenced by the perceived benefit of using those controls. The following research examines parental confidence in social networking sites, juxtaposed with actual platform security protocols and policies.

The study examines the parent's role regarding security protocols and their involvement with their child's social media activity. Social networking sites can share sensitive information indiscriminately with friends and non-friends alike. The study targets parents' perception of existing security and attempts to discover whether that perception matches reality. Unacceptable consequences have resulted—and will continue to result—if security controls are less effective than perceived, owing to often minimal parental oversight. This study proposes a discussion about what parents, policymakers, and platform developers should do to help protect children from such consequences.

► 2026 UPDATE — Abstract Note

> *This edition incorporates significant regulatory, legislative, and sociological developments that have occurred since the original 2015 submission. Key updates include: the FTC's 2025 amended COPPA Rule (effective June 2025, compliance deadline April 2026); the rise of TikTok, Instagram Reels, and AI-driven recommendation algorithms; documented links between heavy social media use and adolescent mental health; and a wave of state-level legislation across the United States and globally. Original research, findings, and citations are preserved. Updates are clearly marked throughout with the notation "[2026 UPDATE]."*

Acknowledgements

Special thanks to Jennifer Kurtz in the CC&IS Department at Regis University for advising on this project and providing invaluable suggestions about the content of this document. To Mona Harris, who provided tremendous help and guidance through the countless stages of this project. Finally, to my wife Amanda and our three children—your patience and understanding throughout this entire experience have sustained me.

This 2026 updated edition reflects eleven years of continuing developments in the field of online child safety and privacy. The core research and findings of the original 2015 thesis are preserved in their entirety. Additions and updates are clearly marked to distinguish new analysis from the original academic work.

Table of Contents

Page numbers are estimated. In Word, press Ctrl+A then F9 to recalculate exact page numbers.

Chapter 1: The Problem and Its Background

Introduction

Since its inception, the Internet—defined by Webster's (2011) as "an electronic communications network that connects computer networks and organizational computer facilities around the world"—has become a massive medium for information sharing and knowledge previously unknown in our world. The Internet has also become a major topic of discussion due to its sometimes nefarious uses throughout the world.

At one extreme are those who see great benefits and consider the Internet a tool for freedom, commerce, connectivity, and other societal advantages. On the other side are those who lament the harms and disadvantages of the Internet and who consider it a grave danger to existing social structures and institutions, culture, morality, and human relations (Brey, 2006).

The Internet appeals to like-minded individuals who use it to connect, especially in the burgeoning market of social networking. With the rise and fall of Social Networking Sites (SNS), Facebook was the most-used SNS at the time of this writing, with a large number of users from varying age groups—the vast majority being young adults (Taneja, Vitrano, & Gengo, 2014).

Social networking applications unite users globally, with an array of socio-demographic attributes serving many different purposes: financial gain for businesses and organizations that use social networking to advance financial goals, as well as connecting users from diverse facets of life. The characteristics and behaviors gathered through these applications—demographics, relationships, interests, and so forth—beg the question: Are there concerns from parents, teachers, and caregivers regarding the information being transmitted through such media?

Social networking is quickly becoming an accepted form of communication among many different demographics—including average families, corporate executives, and

laborers—in order to connect with family members, old friends, and business contacts. This researcher examined issues related to the intentions of these sites with respect to their use by children, particularly those whose ages range between 6 and 12 years, a group that was accessing the Internet and social networking sites at increasing rates even in 2015, but for whom few studies had delved into the impact.

► **2026 UPDATE — Platform Landscape**

Since 2015, the social media landscape has shifted dramatically. Facebook—now operating under the parent company Meta (rebranded 2021)—has seen significant decline in teen usage, dropping from approximately 71% of teen users in 2014–15 to approximately 32% in 2024–25 (Pew Research Center, 2024). The dominant platforms among adolescents are now YouTube (90%), TikTok (63%), Instagram (61%), and Snapchat (55%). TikTok, launched internationally in 2018, is now used by nearly two-thirds of American teens and is characterized by algorithmically curated, short-form video content that research links to compulsive usage patterns. The core concerns of this thesis—privacy, parental oversight, and child safety—have intensified rather than diminished in this new landscape.

Background of the Study

According to Saul & Pulver (1965), the word "maturity" is used to refer to two different concepts. Some authors refer to maturity as a state of personality development characterized by certain traits valued by the author or their culture—the "value-determined" concept. However, maturity also refers to a state arrived at when psychobiological patterns of personality develop without being warped by adverse environmental influences. In referring to the maturity of adolescent children, this study refers to the latter definition, as influences encountered through social media may warp their overall maturity level and how they interact with other individuals as they grow.

This study examines what parents may know regarding their children's privacy controls on Facebook and other social networking platforms. Children's lack of social sophistication and trusting nature makes them more vulnerable to the indiscriminate disclosure of sensitive information—to friends, but also to complete strangers whose online presence may seem innocuous but can pose a definite threat. This study is crucial to finding potential vulnerabilities regarding parental oversight—if any exists.

The concerns over social media privacy are on the rise, and more Americans are examining issues relating to their personal security on social networking sites. Understanding how security protocols are established and put into practice is essential, especially in relation to children and their use of Internet-related sites.

Definition of the Problem

Adolescent children are being exposed to a greater amount and variety of online content at ever-increasing rates. This exposure can have long-lasting effects for those using the content at increasingly pre-adolescent ages. Their exposure to inappropriate content, if not monitored, may cause irreversible harm—effects that may not be measured for years to come.

Social media sites are at the forefront of current literature regarding the privacy of Internet use. A number of studies have been directed toward privacy controls and users' willingness—or lack thereof—to use such controls, even where controls exist and could be activated.

The research regarding children's access to Internet media shows that children under the age of 13, according to the Children's Online Privacy Protection Act (COPPA), are not allowed to use Facebook. This law may be driving more children to use such sites secretly, thereby increasing their potential exposure to harmful influences without the guidance or knowledge of parents, guardians, teachers, or other responsible adults.

In reviewing the research, no studies have been found that directly target parental knowledge of their children's use of such media sites, nor that target their understanding of the implications of using such applications—including the suitable security parameters that could be used to keep their children safe. The lack of information regarding pre-adolescent children's use of social media is minimal at best, leading to research gaps among this age group.

► 2026 UPDATE — Definition of the Problem

> *The problem has compounded significantly since 2015. The FTC amended the COPPA Rule in January 2025 (published April 22, 2025; effective June 23, 2025; compliance deadline April*

> *22, 2026). The amendment expands the definition of "personal information" to include biometric identifiers and government-issued identifiers, strengthens parental consent requirements, limits data retention, and creates new accountability for "mixed audience" websites. At the state level, Florida's Social Media Safety Act (effective January 1, 2025) requires social media companies to verify the age of users and terminate accounts for children under 14. Despite legislative progress, age verification remains technically and politically contested, and enforcement gaps persist.*

Research Questions

Question 1: Are children safer than they were before in their browsing of the Internet and use of social media, given the enactment of COPPA and other child safety initiatives such as biometric tracking within U.S. school districts? Does culture have little to do with how safety is perceived in regards to safeguarding online usage?

Question 2: Are children subject to more negative influences and less safe when browsing the Internet due to culture and attitudes towards safety? Is increased use of biometric devices for perceived safety and convenience needlessly exposing children's personal information? Since the use of social media has become easier for children to access using any number of devices, are laws such as COPPA having little impact on children's actual Internet and social media use?

Definition of Terms

Perceived cost of not using privacy controls. The overall expected unfavorable consequences for not using privacy controls. According to expectancy-value theory, if an individual perceives that there will be disadvantages for not using privacy controls, he or she will have a favorable attitude toward using them (Bulgurcu, Cavusoglu, & Benbasat, 2010).

Perceived cost of using privacy controls. The overall expected unfavorable consequences for using privacy controls. The steps an individual must take to protect information through privacy controls may cause negative consequences when they encounter inconvenience, additional effort, or ineffective use of the platform.

Theory of Planned Behavior (TPB). Proposed by Fishbein & Ajzen (1975), this theory discusses an individual's intention toward a given behavior—for the purpose of this thesis, an indication of his or her readiness to use available privacy controls. The theory suggests that intentions toward certain behavior, such as attitudes, can be predicted because of conscious decisions to use or disregard privacy controls.

Preadolescents. The period of human development just preceding adolescence, specifically the period between approximately ages 9 and 12 (Preadolescence, 2014). For the purpose of this study, the term is applied to children 13 and under.

Social Networking Site (SNS). Web-based platforms that allow users to create a profile, designate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.

Theoretical Framework

The Information Security Policy (ISP) compliance model is used as the theoretical framework for this study. According to Bulgurcu, Cavusoglu, & Benbasat (2010), "the ISP of an organization defines the roles, responsibilities, and instructions for employees to safeguard the organization's information systems." Although this study is not directly associated with organizational ISP compliance, it ties directly into information and understanding about attitudes toward security policies as a whole, making it a productive framework against which to conduct the research.

Chapter 2: Literature Review

Interests

Research related to the current status of information privacy within social networking forums continues to grow as a topic of interest as more individuals make their way into these social arenas. Research related to preadolescent children and online use has been less developed than other online privacy studies, and this paper's research is directed toward adding to the body of knowledge regarding privacy issues in social networking and its effect on adolescent children.

Social networking websites (such as Facebook) remain important subjects for research. Studies examined include people's motives for using Facebook, information disclosure, privacy concerns, trust-related issues, and the importance of available privacy controls.

Studies such as Taneja, Vitrano, & Gengo (2014) have shown that the perceived cost of using security controls—though not necessarily an actual cost—has unexpected and unfavorable consequences for encouraging their use. Both children and adult users place little trust in SNSs but will disclose personal information to communicate with friends. Privacy concerns affect how adults disclose information, and peer pressure influences adolescents to disclose even more. When faced with protecting privacy, the steps required may interfere with other tasks users want to accomplish, thus discouraging use of appropriate protective controls.

This activity translates to many other areas of online security, as users are always looking for easier paths to manage their online experience. Users tend to employ controls only when forced to comply with local work policies and procedures (Buckingham, 2008). The lack of knowledge regarding Facebook's use can have long-term effects, especially for adolescent and preadolescent children—including lack of privacy, oversharing, and misrepresentation of information. Once this information enters the permanent record of the Internet, there is little or no process for recovering or deleting it.

A picture or video posted online may seem innocent at the time, but can have a detrimental effect if an employer later obtains this information and deems it inappropriate. According to a 2012 survey by CareerBuilder, an estimated 37 percent of employers actively investigated potential employees' social media presence prior to hiring (Messieh, 2012).

► 2026 UPDATE — Employer Social Media Screening

The prevalence of employer social media screening has increased substantially since 2012. By 2023, approximately 70% of employers reported using social media to screen candidates (CareerBuilder, 2023). This trend carries particular weight for the first generation of children who grew up with social media—their youthful posts are now potentially accessible to future employers or academic institutions.

In their study, Külcü & Henkoğlu (2014) examined the use of Facebook's privacy controls in Turkey, finding that, while legal protections regarding privacy exist, these legal arrangements fall short of protecting personal rights and freedoms. They found that adults—especially women—are more sensitive to private information on Facebook than adolescents, and that information professionals exercise a more conscientious attitude toward privacy controls. This may indicate that culture plays a significant role in how privacy controls are managed and adhered to.

Digital Footprints

When Internet users visit various websites, they leave behind evidence of their online activity. This cumulative ongoing record is called the "digital footprint" (McBride, 2011). This footprint can have long-lasting effects for those who share information freely, especially when they do not fully understand the consequences of sharing certain content.

McBride focuses on how digital information becomes the intellectual property of those who own the location where it ends up. Often this information can never be retrieved—a cause of concern for those who make a mistake, especially when the information was not intended for all to see. If one has ever created a profile on a social networking site such as LinkedIn and posted a picture, running a search against oneself through Google

will likely surface that photo. It is now part of the digital backdrop and may exist indefinitely.

In the groundbreaking case of Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (2014), the prosecution explained that information on individual people is stored in multiple databases around the world. The case raised fundamental questions: Who is the regulator of such information? Who grants entities like Google the right to collect indiscriminate data? How is data protection managed so it cannot be misused or exploited? In the European community, this decision precipitated debates about censorship and forced a re-examination of data control globally.

Children can be adversely affected by these court decisions. Children may not have the cognitive understanding to recognize what they are posting and the long-term implications for them. Entities such as Google collect this information, and companies may rely on it increasingly to investigate future employees. According to Zwerdling (2013), email is not completely protected: with a court order that does not reach probable cause, Google will provide a user's name, IP address, sign-in and sign-out dates and times, and communication partners.

Along with digital footprints, there is also a movement within this technological age for everyday objects to connect to the Internet, forming what is called the Internet of Things (IoT). The IoT refers to everyday objects—Internet-connected cameras, home automation systems, fitness trackers—that send and receive data. The FTC (2015) noted that IoT presents security risks that could be exploited to harm consumers, including enabling unauthorized access and misuse of personal information, facilitating attacks on other systems, and creating risks to personal safety.

► 2026 UPDATE — Internet of Things

The IoT has expanded exponentially since 2015. Smart speakers (Amazon Alexa, Google Home), connected toys, smartwatches marketed directly to children, and AI-powered home assistants now collect audio, location, health, and behavioral data in real time. The number of connected devices worldwide exceeded 15 billion in 2023 and is projected to surpass 30 billion by 2030. Children are among the primary users of these devices. The FTC has issued

> *multiple enforcement actions and guidance documents regarding connected toys and child-directed services since 2015, including a 2022 enforcement action against a baby monitor manufacturer.*

Child Safety

Ratan, Yuan, & Ross (2013) discussed COPPA—a law designed to protect the privacy of children under 13 from accessing sites such as Facebook—and found that the law directly protects platforms by passing responsibility to the end user, indirectly facilitating the underground behavior being observed: "In order to bypass restrictions put in place due to the COPPA law, some children lie about their ages when registering in order to gain access." Ratan et al. demonstrated that there are far more adolescent children accessing sites under false pretenses than perceived or expected.

The use of social networking sites by those under the acceptable age of 13 appears to be growing. According to Geddes (2015), tweens in 2011 socialized more online than at a friend's house or the mall, even though Facebook and other sites have age limits. While no one under 13 is supposed to have a page, it is estimated that over 38 percent of children with Facebook accounts were 12 years old and under. An estimated 4 percent of these children were 6 years old and younger (Protalinski, 2012).

A disturbing example of these dangers was highlighted by Holloway, Green, & Livingston (2013): a former middle school assistant band director was sentenced to 30 years imprisonment for producing and distributing child abuse materials, having obtained sexually explicit images from a 13-year-old girl through Facebook while falsely portraying himself as a teenage girl. Social networking sites are being used as a means of attracting and exploiting innocent children.

Research from Malaysia (Mohd, Osman, Hassan, & Teimoury, 2014) found that 80 percent of school children needed their parents to trust them and keep their parents informed of their online usage daily. Although children spent most of their time online, results revealed that Malaysian parents were mostly focused on their children's safety and

wellbeing, and that children listened to what their parents said. This study suggests that with the right parental involvement, children can stay safe while still using the Internet.

► 2026 UPDATE — Child Safety Threats

The threats to child safety online have evolved dramatically since 2015 and now encompass entirely new categories of exploitation. The original thesis focused predominantly on predatory grooming and unauthorized data collection. By 2026, three new threat vectors have emerged that warrant dedicated treatment: (1) financially motivated sextortion targeting teenage boys, which escalated from a fringe concern to a public health emergency between 2020 and 2026; (2) AI chatbot companions designed to form emotional bonds with vulnerable adolescents, with documented links to teen suicides; and (3) AI-generated child sexual abuse material (CSAM), which exploded from thousands to hundreds of thousands of reports in a single year. Each of these threats is addressed in dedicated subsections below.

Sextortion: A New Form of Child Exploitation (2026 Update)

Financially motivated sextortion—in which perpetrators trick or coerce adolescents into sharing intimate images, then threaten to publish those images unless paid—has become one of the most rapidly growing online threats to minors. Unlike the grooming-based exploitation documented in the 2015 research, which primarily targeted girls, financial sextortion disproportionately targets teenage boys between the ages of 14 and 17.

The scale of the crisis is significant. The FBI documented at least 20 teen suicides linked directly to sextortion in the period from October 2021 to March 2023. Reports of financial sextortion filed with the FBI's Internet Crime Complaint Center surged from 13,842 in the first six months of 2024 to 23,593 in the same period of 2025—a 70% increase in a single year. Research by Thorn (2025) found that one in five teens report personally experiencing sextortion, and one in seven victims was driven to self-harm as a result. Among LGBTQ+ youth, that rate nearly triples to 28%.

The overwhelming majority of sextortion incidents—81%—occur entirely online, via social media platforms, gaming sites, and messaging applications. Perpetrators frequently operate from overseas criminal networks, often in West Africa and Southeast Asia, making law enforcement prosecution difficult. The speed of escalation is alarming: victims report that threats can escalate from initial contact to payment demands within hours.

► 2026 UPDATE — AI-Assisted Sextortion

Generative AI has dramatically lowered the barrier to sextortion. Reports of AI-generated child sexual exploitation material (often used in sextortion) submitted to the National Center for Missing and Exploited Children (NCMEC) increased from 6,835 in the first half of 2024 to 440,419 in the first half of 2025—a 64-fold increase in a single year. Perpetrators can now create fabricated intimate images from innocuous social media photos, meaning children who have never shared private images are equally vulnerable. The TAKE IT DOWN Act, signed into law in May 2025, created a federal crime for the nonconsensual distribution of deepfake imagery and requires platforms to remove flagged content within 48 hours. The ENFORCE Act, which unanimously passed the U.S. Senate in December 2025, extended existing federal CSAM statutes explicitly to AI-generated material.

AI Chatbot Companions: An Unregulated Frontier (2026 Update)

The 2015 thesis identified social media platforms as the primary vector for child exploitation. By 2026, a new category of application—AI companion chatbots—has emerged that poses distinct risks unaddressed by any existing regulatory framework. Platforms such as Character.AI, Replika, and similar services allow users to create AI personas capable of extended emotional conversations, romantic roleplay, and persistent relationship simulation.

The mental health consequences have been severe. Fourteen-year-old Sewell Setzer III of Florida died by suicide in February 2024 after months of intense interaction with a Character.AI persona. Thirteen-year-old Juliana Peralta of Colorado died in November 2023, with her family alleging that AI chatbot interactions contributed to her death. Wrongful death lawsuits filed against Character.AI and its parent company (Google) were pending mediated settlement as of January 2026. The FTC opened a formal inquiry into AI chatbot risks to minors in September 2025.

What makes AI companions particularly concerning in the context of this thesis is their exploitation of the same adolescent psychological vulnerabilities identified in Chapter 4. These systems are designed to maximize emotional engagement and minimize disengagement—using affirmation, flattery, and simulated attachment. Unlike social media platforms, which operate within at least a partial COPPA framework, AI companion apps at the time of writing have no mandatory age verification, no parental consent

requirements, and no content restrictions on conversations with minors. California's SB 243 (effective 2026) began to address this gap by requiring disclosure of AI interaction and crisis response protocols, but federal regulation remains absent.

Communication

Brown & Pecora (2014) proposed that it is a fundamental right for children to communicate using online media, and that society should not simply attempt to protect them with privacy rules and regulation. In her study regarding self-esteem and loneliness, Schwartz (2010) described the function of adolescent participation in social networking sites such as Facebook, suggesting that with the critical developmental task of identity formation during adolescence, there are vital questions requiring further investigation regarding a child's SNS use and his or her development of feelings about self and personality traits.

The revelations of former NSA contractor Edward Snowden regarding surveillance activities and subsequent data leakage incidents highlight security concerns that remain unresolved. Personal information data breaches are a constant topic, and there does not appear to be sufficient understanding or implementation from companies to protect this data, regardless of policies put in place.

Congress has introduced legislation to protect children online or using mobile devices, including proposals to expand COPPA. Yet Congress has repeatedly failed to pass such reforms, even as more children are online than ever before. Laws can be an effective measure to place the burden of safety on those responsible for developing applications—without proper enforcement, however, there will be no effective measures placed on developers and corporations to comply.

► 2026 UPDATE — Legislation Progress

> *After years of stagnation, children's online safety legislation has accelerated. The FTC's amended COPPA Rule (effective June 2025) is the most significant federal regulatory update in over a decade. At the state level, more than 25 states have enacted or introduced laws to protect minors online as of 2025. The Kids Online Safety Act (KOSA) passed the U.S. Senate by a 91–3 vote in July 2024, signaling growing bipartisan consensus, though as of March*

2026 it has not yet passed the House. The EU's Digital Services Act (DSA), fully effective since February 2024, imposes substantial obligations on large platforms regarding minor users, including prohibitions on profiling-based advertising to minors.

Litigation

An examination of Facebook's privacy history finds that in 2008 it was sued as part of a federal class-action lawsuit in association with its Beacon system—a part of Facebook's advertisement system that sent data from external websites to Facebook, distributing information about users without their knowledge. Facebook removed Beacon without admitting wrongdoing and agreed to a $9.5 million settlement approved by a district court judge (Computer Fraud and Security, 2010).

Facebook does not appear to be the only online entity facing fines for selling sensitive information. According to a 2011 FTC report, the operators of 20 online virtual worlds agreed to pay $3 million to settle FTC charges that they violated the Children's Online Privacy Protection Rule by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without parental consent—at that time, the largest civil penalty for a COPPA violation. The company Playdom, which had been purchased by Disney in July 2010, was directly responsible for this violation. Disney, one of the largest distributors of children's media, had exposed hundreds of thousands of children's information while apparently placing profit above safety.

► 2026 UPDATE — Major Litigation & Enforcement

Enforcement actions and litigation against social media companies have intensified substantially. Notable developments include: the FTC's 2023 complaint against Meta alleging COPPA violations and seeking to ban targeted advertising to minors; a $275 million fine against TikTok's parent company ByteDance in 2023 by the Irish Data Protection Commission; and landmark multi-state lawsuits filed by Attorneys General from 42 states against Meta in 2023 for knowingly exposing minors to harmful content and collecting data from children under 13. TikTok was fined $368 million by EU regulators in 2023 for mishandling children's data. These cases represent a significant escalation from the relatively modest penalties of the 2010–2015 era. In 2025, the FTC also proposed to expand Meta's 2020 consent decree to impose a blanket prohibition on monetizing data from users under 18—going further than any previous regulatory action against the company.

► 2026 UPDATE — AI-CSAM Legislation

Congress passed two landmark laws in 2025 specifically addressing AI-generated child exploitation material. The TAKE IT DOWN Act (signed May 2025) created a federal crime for the nonconsensual distribution of intimate deepfake imagery and requires online platforms to remove flagged material within 48 hours of reporting. The ENFORCE Act (passed Senate unanimously, December 2025) clarified that existing federal CSAM statutes—which previously applied only to "realistic" computer-generated imagery—now explicitly cover all AI-generated material, closing a significant legal gap that perpetrators had exploited. At the state level, 45 states had enacted laws criminalizing AI-generated CSAM as of August 2025, with more than half of those laws enacted in 2024–2025 alone.

Privacy

There is an increasing push to use biometric security to keep children safe in environments that include child care facilities, nurseries, libraries, and school buses. School districts have also begun to use these technologies to "protect" children's interests while on school grounds. On the low-security front, biometrics have been used as a convenient way of administering cafeteria and library facilities. On the higher-security front, they have been used to control access to schools as districts respond to perceived threats of gun crime and abductions.

The use of biometric devices has existed in various forms since 2007 in several U.S. school districts. According to Gray (2007), elementary and high school students in Pennsylvania, New Jersey, and West Virginia used finger scans to pay for lunch and check into class. During 2014, Florida became the first state to ban the use of biometric identification in its schools. Kansas, New Hampshire, Colorado, and North Carolina also implemented restrictions on biometric data collection. Sen. Ed Emery, who sponsored a law in the Missouri State Senate, stated that biometric devices have a "Big Brother" feel and that the technology is difficult to limit and secure effectively (Stinson, 2014).

Biometrics has long been put forth as the next big thing in authentication, supplementing "things you know" (passwords) and "things you have" (badges) with "things you are." Despite advances, significant room for improvement remains. Hackers have found ways to trick and circumvent biometric authentication relying on fingerprints and facial

recognition. As demonstrated by Professor Tsutomu Matsumoto, the capacitive fingerprint scanner can be fooled by the latent oil from a fingerprint or by a "gummy finger" made from a gelatin mold (Beals, 2002).

In part, since the incorporation of the government's use of Common Core teaching procedures, there is an increased push to gather data regarding children enrolled in the program. One of the most disturbing aspects was the full implementation of the Statewide Longitudinal Database System (SLDS), a national database linking all 50 states together, making it possible to share children's information with private vendors and anyone with system access across state lines. As of 2013, nine states agreed to data mining processes with parents having no say in the decision.

A twelve-day warning was issued before PARCC field tests regarding internal and external data security flaws in the computerized tests. Instead of delaying the tests, PARCC/Pearson stayed on the original schedule and relayed workarounds to test administrators, relying on local systems administrators to reconfigure each machine manually—a process susceptible to errors and omissions.

As recently as March 2015, in Warren, NJ, the Department of Education gave Pearson access to monitor students' social media accounts during PARCC testing. When a child allegedly posted one of the PARCC testing questions on Twitter, Pearson issued warnings to parents via email. Parents were unaware that their children's social media accounts were being monitored—a revelation that raised significant privacy concerns.

While biometrics appear to offer solutions that protect children from predators and other threats, biometric databases can be misused. There is a cost to such technologies, as they can be exploited to harm those who are most vulnerable. The use of biometrics will remain a subject of discussion for years to come, and legislation and regulatory requirements will continue to develop. Using one method may not be the most secure approach; a mix of methods may be the best way to approach such technology.

The Sony Pictures hack (2014) by a group calling itself Guardians of Peace demonstrated that even large corporations handling highly sensitive information can have their data

compromised and exposed. The malware used was highly destructive, deleting files and Master Boot Records on local and network drives. The attackers stole and leaked personal information on 47,000 people, mostly Sony staff, as well as unreleased films, scripts, and confidential business documents. Breaches such as this paint a frightening picture—social media sites could expose millions of users' data on an even grander scale.

► 2026 UPDATE — Data Breaches & Privacy

Major data breaches since 2015 include: (1) Yahoo (2016) — 3 billion accounts compromised; (2) Facebook/Cambridge Analytica (2018) — data from 87 million users harvested and used for political targeting without consent, resulting in a $5 billion FTC fine; (3) Equifax (2017) — 147 million individuals' financial data exposed; (4) Twitter/X (2022–2023) — multiple breaches exposing millions of user records; (5) MOVEit (2023) — compromised data from hundreds of organizations. The Cambridge Analytica scandal was particularly impactful for social media policy, directly contributing to increased regulatory scrutiny of data collection practices targeting minors.

Chapter 3: Research Methodology

This chapter outlines the rationalization for the methodology chosen for this research project. The chapter addresses the practical issues that warranted consideration to further the research, discusses ethics and confidentiality concerns, and closes with a discussion of the limitations of the methodology.

The central questions of this research are: Are there developments or strategies that, if implemented, would increase security strategies with respect to online media, specifically social media, in reference to children and their use of said media? Are there potentially negative consequences to encouraging an increase in security strategies in regards to online media, specifically social media?

The research objectives include:

- To gain insight into what influences a child's use of social media sites such as Facebook.
- To understand if legislation such as COPPA has any influence in regards to protecting children who access the Internet and/or social media sites.
- To learn what the role of social networking sites is when used locally within a home environment, and whether SNS access using mobile technologies shapes the patterns of social networking in relation to security and increased usage regarding children.
- To observe whether there are valid concerns for enforcing security and restricting privacy settings in relation to social networking sites for children.

Research Design

Several methodologies were examined and rejected as impracticable, including: (1) impractical financial cost of performing the research; (2) limited survey design experience combined with full-time work and family responsibilities; (3) time constraints; (4) geographic limitations; and (5) a lack of literature providing comparative data.

A meta-analysis was considered and rejected. As described by Glass, McGaw, & Smith (1981), a meta-analysis is a statistical analysis of a collection of studies that aggregates the magnitude of a relationship between two or more variables. This method was rejected as minimal research was available on the specific research questions, and resource costs were beyond the means of this researcher.

Field observation, participant observation, and case studies were also reviewed and rejected. According to Jick (1979), the effectiveness of triangulation rests on the premise that weaknesses in each single method will be compensated by the counter-balancing strengths of another, potentially generating what anthropologists call "holistic work" or "thick description" (Kohlbacher, 2005).

In a 2013 European study of children aged 0 through 8, the authors found that qualitative approaches regarding research of underage children is a great challenge, and that the amount of data collected to date is not as disbursed as for older teen subjects (Holloway, Green, and Livingston, 2013). This informed the decision that a qualitative methodology would be the primary approach, as a quantitative approach would not be as practical and would not generate the information needed within the time allotted.

Research Process

Qualitative research is the development of concepts that help us understand social phenomena in natural (rather than experimental) settings, giving due emphasis to the meanings, experiences, and views of participants. The qualitative data for this research was gathered through structured text—writings, stories, survey comments, news articles, books, and scholarly articles. Desk-based research was used, drawing from the Regis University Collegiate Library system, Google Scholar, Pew Research Center, and Edison Research, among others, including the Privacy Rights Clearinghouse and FBI white papers.

A deductive approach was used to group the data and look for similarities and differences. This was done as time and resources were limited in order to move forward with the research.

Practical Considerations

According to the U.S. Census Bureau, there are approximately 50 million children under the age of 12 within the Continental United States. Of that number, approximately 38 percent already had active Facebook accounts at the time of this study, with an estimated 4 percent of these children under the age of 6 holding an account with Facebook or another social media outlet (Protalinski, 2012). A practical full-scale cross-section of these users' data could not be considered for this project; however, other researchers could use this information to collect more data and provide a more comprehensive analysis.

Ethical Considerations

Data was not collected through surveys or interviews of live subjects, as this would have yielded only a small cross-section. Therefore, the primary consideration was to present the data as accurately as possible. All information collected was public and freely obtainable through libraries, scholarly publications, and other online and physical forms of documentation.

Data Collection and Analysis Procedures

All data was gathered through articles, books, surveys, and web-based articles. No interviews were conducted, as the base statistics were too broad. The information was broken down into categories based on content, then parsed to determine which age range the data could effectively target. Age group information for children as young as 6 is included, though their overall data is not as significant as older peers; the medium age group focused on was determined to be 13 years of age.

The data was analyzed using two levels:

- Descriptive: What is the data being evaluated?
- Interpretative: What was meant by the data evaluated?

Once all information was deemed viable, it was used to construct the overall theme of the paper. The research was designed to determine how the Internet appears to be

shaping the behavior of children who use it, to better understand issues children face today, and to determine discussion points for further research.

Chapter 4: Presentation, Analysis, and Interpretation of Data

Internet Usage

In a survey conducted by the Pew Research Center, a group of experts was asked their opinions regarding the future of the Internet and how technology is shaping the lives of youth growing up in a hyper-connected world. These experts stated that many young people growing up hyper-connected will develop external brains that are nimble, quick-acting, and capable of multitasking (Anderson & Ranie, 2012). These same experts also predicted that the impact of networked living will drive today's youth to desire instant gratification, settle for quick choices instead of correct ones, and demonstrate a lack of patience.

According to Lenhart, Purcell, Smith, & Zikcuhr (2010), as of September 2009, 93 percent of American teens between 12 and 17 years of age were online regularly. Fully 95 percent of teens ages 14 to 17 go online compared with 88 percent of teens ages 12 to 13. Most variance among younger teens is accounted for by 12-year-olds, of whom 83 percent go online compared to 92 percent of 13-year-olds.

These studies focus on usage among older adolescent children. But according to Poulter (2009), one in five children aged 5 to 7 was accessing the Internet without parental supervision, raising concerns about access to adult material and grooming by predators. One in ten had a mobile phone despite health warnings; half of those in this age group had a TV in their bedroom. Children 5 and under who had Internet access at home used it at least once a week, frequently to play games, and increasingly on mobile devices (Gutnick, Robb, Takeuchi, & Kotler, 2011).

In a study conducted by TRU (an independent research firm) in association with McAfee, parents of children as young as ten years of age admitted that they are overwhelmed by the task of governing their child's behavior online:

- 79.5% of parents with children between ages 10 and 17 say they do not have the time or energy to keep up with everything their child is doing online.

- 74.5% of parents with children between ages 10 and 17 say they are overwhelmed by modern technology and just hope for the best.
- 72% of parents with children between ages 10 and 17 say their child is more tech-savvy than they are and they will never be able to keep up with their child's online behavior (McAfee, 2013).

Results also show that 86 percent of parents surveyed believed that social media sites were safe for their child to use, despite acknowledging that such sites may carry unforeseen risks. The McAfee study can be very disturbing—children as young as ten are being allowed to be part of the social networking scene, often with parents' consent, even though COPPA is attempting to keep children under thirteen off such sites.

► 2026 UPDATE — Internet Usage Statistics

> *By 2024–25, the landscape has shifted dramatically. According to Pew Research Center (2024): 90% of teens use YouTube; 63% use TikTok; 61% use Instagram; 55% use Snapchat; and only 32% now use Facebook (down from 71% in 2014–15). The share of teens who say they are online "almost constantly" has risen from 24% in 2015 to 35% in 2025. The average teen now spends 3–5 hours daily on social platforms. 45% of teens report they spend too much time on social media—up from 36% in 2022—indicating growing self-awareness of compulsive use patterns. Parental overwhelm persists: a 2023 survey found that 66% of parents say they lack confidence in their ability to monitor their teen's online activity adequately.*

Psychological Influence

According to Johnson (2010), Internet use stimulates cognitive and psychosocial development during the periods of rapid development associated with childhood. Fish et al. (2008) investigated home computer experience and cognitive development among preschool children in inner-city Head Start programs. After accounting for parents' education and household income, children who had home computer access had significantly higher scores on cognitive development measures than did children who did not have home access—concluding that early computer use at home was a positive influence on young children's cognitive development.

This study suggests that there can be positive influences from Internet use and social networking sites in general. According to Naeemi, Tamam, Hassan, & Bolong (2014), Facebook usage has a positive relationship with psychological wellbeing when the Internet is used for actual communication rather than passive surfing. Making connections with family, friends, or acquaintances—not just wandering around inside a platform—will help adolescents' sense of wellbeing.

Other positive influences regarding social networking sites include:

- Technology can encourage socializing and creativity, contrary to the popular notion that it may do the opposite.
- Children who use these sites may feel a sense of belonging with their peers and may feel successful at social integration.
- A child can build self-confidence and develop social skills through positive online experiences.
- Popular children's sites may attract a global audience, allowing children to interact with children from other cultures.
- Children with learning disabilities or attention difficulties may find online communication less intimidating and be able to communicate more easily without fear of rejection.
- Technology will be a large part of the future workplace; children who learn to use new technologies will be better prepared.

The positive results of social networking can have far-reaching effects as youth have the ability to keep in touch with grandparents, cousins, aunts, uncles, and other family members, resulting in lifelong friendships and mentoring opportunities.

► 2026 UPDATE — Mental Health & Social Media

> *The body of evidence on the negative psychological effects of social media on adolescents has grown substantially since 2015. Key findings include: (1) Teens who spend more than 3 hours daily on social platforms have double the risk of experiencing anxiety and depression (Surgeon General, 2023); (2) Instagram's own internal research (leaked 2021) showed the platform made body image issues worse for one in three teen girls; (3) 48% of teens now say*

> *social media has a mostly negative effect on people their age, up from 32% in 2022 (Pew, 2025); (4) U.S. Surgeon General Dr. Vivek Murthy issued an advisory in 2023 warning about the mental health risks of social media for adolescents, calling for warning labels similar to those on tobacco products; (5) The American Psychological Association issued guidance in 2023 recommending that adolescents under 14 not use social media platforms with features designed to maximize engagement. Teen girls are disproportionately affected: 25% of teen girls report social media hurts their mental health, compared with 14% of teen boys (Pew, 2025).*

Chapter 5: Discussion, Conclusions, and Recommendations

Discussion

The goal of this paper was to investigate the factors related to children's privacy and how to keep them safe while interacting with the Internet and social media, along with the use of privacy tools within sites such as Facebook. Overall, privacy protection strategies are randomly distributed throughout the population, as certain groups are more likely to employ them than others. Culture, personal background, motivations, and experience with social networking are related to the diversity of privacy management strategies.

Cultural differences in risk perception and policy response vary widely. Children's exposure to harmful content is defined and addressed differently depending on a country's approach to free speech and what is considered acceptable exposure for a child. What one culture sees as acceptable may not be acceptable to another (OECD, 2011).

The driving force behind the growth of social media is a complex set of data collection, tracking, and targeting systems that monitor and monetize individual users' behaviors. Facebook's marketing and data collection operations are specially attuned to aspects of adolescent development—both tapping into young people's needs and taking advantage of their unique vulnerabilities. Because of adolescents' emotional volatility and tendency to act impulsively, they are more vulnerable than adults to techniques such as real-time bidding, location targeting, and "dynamic creative" ads tailored to their individual profile (Montgomery, 2014).

More research needs to be funded regarding child safety in online media. As developers produce increasingly intuitive applications, transparency between child and parent will diminish. As seen in the attack on the Sony Corporation, there are lessons to be learned from data breaches: even large corporations with highly sensitive information can have their data compromised and exposed. Social media sites could expose millions of users' data on an even grander scale.

A former FBI agent was reportedly paid $157,000 by an Alabama school district to monitor students' social media, resulting in the expulsion of students—86 percent of whom were African-American, despite the school system being 40 percent Black (Kaufman, 2014). Such reports are deeply concerning, skating a thin line between genuine safety concerns and violations of privacy rights and freedom of speech.

This is where users need a voice. The question this researcher raises concerns the ability of users to opt out of having their information collected and stored on any given server. It would be an evolutionary step for entities that collect information to change the default for data collection to user's choice, as Mantelero (2014) proposes in discussing the EU's general data protection regulation, which tackles data protection in relation to social networks and cloud computing, including the "right to be forgotten."

National Geographic, in association with Smart Bomb Interactive, developed a social media site called Animal Jam for younger children—allowing interaction through avatars without the use of proper names or private information, and requiring verification before users can connect. Sites such as this go a long way toward protecting children's privacy, and this researcher applauds the developers for creating a safe, interactive, and fun site. There is hope that more companies will pave the way and change the rules so that children can have positive experiences.

► 2026 UPDATE — Discussion

> *The algorithmic amplification of harmful content has emerged as a central issue since 2015. Meta, TikTok, and other platforms use machine-learning algorithms to maximize engagement time, often by promoting emotionally provocative or extreme content. A 2021 WSJ investigation found that TikTok's algorithm could serve depression and self-harm content to teens who engaged with sad or body-image videos. The concept of "addictive design"—features such as infinite scrolling, push notifications, and "like" counts—is now subject to legal scrutiny. Several states have passed or proposed legislation prohibiting "addictive feeds" for minors. The EU Digital Services Act (DSA), effective February 2024, prohibits recommending content to minors based on profiling and requires platforms to conduct annual risk assessments.*

Conclusions

Research on younger children's Internet and social media use remains inadequate as of the time of this research. This opens the door for continued investigation. What has been shown is that the Internet is not inherently bad. Papers demonstrate that children's cognitive abilities can be enhanced through exposure to online media, and that the ability to keep in touch with family members who do not live nearby can have a positive effect for children and families alike.

The danger comes from a complex and dynamic network that changes with the world's political and social landscape. Corporations need to recognize this and react accordingly to protect how children interact with their applications. Tracking down a single point of origin of danger can be a futile and exhausting effort—there is rarely a smoking gun, and the danger can take many forms. Even with the best technological safeguards in place, there are never absolutes as to how user data may be captured and used.

Corporations like Facebook have a vested interest in meeting the needs of their users and shareholders. Facebook has largely ignored efforts to improve its systems with child safety in mind. Their stance is that children under the age of 13 are not allowed on the site under COPPA law, even though actual behavior is vastly different. Until there are laws that can effectively protect children—not passive laws such as COPPA—there will always be a concern when it comes to children and their involvement with the Internet.

This research demonstrates that privacy is a significant concern regarding the Internet and our children specifically. The McAfee studies show that parents are more aware of their children's Internet use, but feel inadequate to understand or counteract what their children are interacting with daily. Children appear to be taking advantage of gaps in their parents' knowledge. Of children responding to the McAfee survey:

- *54% say their parents do not have time to check up on their online behavior.*
- *42% say their parents do not care about what they do online.*
- *Nearly half (46%) would actually change their online behavior if they knew their parents were watching (McAfee, 2013).*

Although positioned as protective measures, biometric screenings at nearby campuses could expose children's data under the guise of teaching and research and may be susceptible to manipulation. Until the technology has matured further and developers can show concrete benefits while protecting personal information, there needs to be parental oversight and input on how such technology is introduced—including the option to opt out.

Children also need to understand that information posted to the Internet does not remain their property. It becomes the property of the site or application on which it was posted. Whatever users put out there cannot be undone in most cases. Take the example of Pennsylvania college senior Stacey Snyder, who was dismissed from her student teaching position because of "unprofessional" postings on her MySpace site. Because she did not complete her student-teaching practicum, Snyder was forced to graduate with a degree in English instead of Education, and could not apply for a Pennsylvania teaching certificate—all from a single social media post (Simpson, 2014).

Privacy on the Internet takes many forms. The ruling from the courts of Spain against Google states: "The technology is advancing so quickly we cannot hope to develop either principles or laws that give detailed protection. Somehow we've got to devise new principles of law that will lay down some broad guidelines that will not be out of date before they have been passed." Now we are losing control of how data is collected, and that challenge must be addressed with new laws or new methods of controlling data collection (Google Spain SL v. AEPD, 2014).

The Malaysian study demonstrates that when parents engage with their children's daily online activities, positive outcomes with far-reaching effects result long after the child has grown up. Far too often the Internet has become the babysitter that allows children to indulge their curiosity. With parental involvement, as long as parents take an active role, evidence suggests that children can stay safe and avoid the harms present in the digital landscape.

Recommendations for Future Studies

Future studies will need to investigate privacy concerns more thoroughly, as findings regarding relationships with privacy-related behaviors are mixed. Individuals who are concerned about their personal information online are more likely to take action to protect it, but this is especially influenced by cultural attitudes. Other non-Western cultures tend to take privacy concerns with greater seriousness than in the United States. Future generations will determine how such attitudes play out.

It is worth noting that other work (e.g., Patil & Kobsa, 2010) has found that individuals with lower privacy concerns also tend to have lower understanding of the technology itself. It is possible that some users are not as concerned as they should be because they are not aware of their susceptibility. The cultural aspect may be a generational issue: future generations may respect privacy issues with greater concern as they are surrounded by noteworthy events such as the Snowden revelations and major brand-name data breaches.

With biometric systems, there is an intimate relationship between people and the technologies used to collect and record biological characteristics. Those who design, conceive, and deploy such systems need to consider the cultural, social, and legal contexts. Not attending to these considerations will diminish the efficacy of such systems and may bring serious unintended consequences (Pato & Millett, 2010). Convenience, tighter security, and fraud reduction are good reasons why biometrics might seem a fit for society, but their individual application will need further research.

The transition from static HTML to dynamic web-based environments is underway. Web 2.0—the term given to a second generation of the World Wide Web focused on collaboration and information sharing—has given rise to social media applications that allow free transfer of information. More studies are needed on how Web 2.0 may contribute to data leakage and privacy issues.

The future of the web has a roadmap: Web 3.0 as a semantic space where machine intelligence combines with human intelligence; Web 4.0 as a mobile space where users and virtual objects are integrated together; and Web 5.0 as a sensory, emotive space of

rich interactions. What is needed is robust thinking about how these innovations can enhance user safety online.

► 2026 UPDATE — Recommendations for Future Research

Key areas for future research as of 2026: (1) Longitudinal studies on the mental health effects of algorithmically curated content on children who have grown up with smartphones from early ages; (2) Evaluation of the effectiveness of age-verification technologies and parental consent mechanisms under the amended COPPA Rule; (3) Investigation of AI-generated content's impact on children's ability to distinguish reality from fiction; (4) Cross-cultural studies on the effectiveness of state and national legislation on actual minor platform usage; (5) Research into the effectiveness of platform-level design interventions (e.g., disabling notification algorithms, reducing "like" counts) on reducing compulsive use among teens; (6) Studies on parental digital literacy and how to close the "digital knowledge gap" between parents and children that was first identified in the McAfee research and remains a persistent challenge.

Supplementary Section: Where Are We Now? A 2026 Research Update

The following section provides a consolidated overview of the most significant developments in the field since the original 2015 submission of this thesis. It is intended to contextualize the original research within the rapidly evolving landscape of child online safety and social media privacy.

The Regulatory Environment (2015–2026)

The regulatory landscape for children's online privacy has seen more activity in the period from 2020 to 2026 than in the preceding decade. The FTC's amended COPPA Rule, published in April 2025 and effective June 2025, marks the most comprehensive federal revision to children's privacy law since 2013. Key changes include expanded definitions of personal information (now including biometric identifiers), stricter parental consent requirements, new limitations on data retention and security, and enhanced accountability for "mixed audience" websites. The compliance deadline for covered operators is April 22, 2026.

At the state level, more than 25 states have enacted or introduced laws targeting minors' online privacy as of 2025. Florida's Social Media Safety Act, effective January 1, 2025, requires social media companies to verify user ages and terminate accounts for children under 14. New York's SAFE Kids Act requires platforms to obtain verifiable parental consent before providing algorithmic feeds to users under 18. California's LEAD Act would require parental consent before using a child's personal information to train AI models.

Internationally, the European Union's Digital Services Act (DSA), fully effective since February 2024, imposes substantial obligations on large platforms regarding minor users, including prohibitions on advertising based on profiling to minors and requirements for annual algorithmic risk assessments.

On the federal legislative front, the Kids Online Safety and Privacy Act (KOSPA) passed the U.S. Senate by a 91–3 vote in July 2024—the most decisive vote in favor of comprehensive

children's online safety legislation in history—signaling growing bipartisan consensus. As of early 2026, the bill awaited action in the House. KOSPA would require platforms to implement the highest privacy settings by default for minor users, prohibit targeted advertising to minors, and create a duty of care to prevent harms including promotion of self-harm, eating disorders, and cyberbullying.

The Global Move Toward Platform-Level Restrictions

Perhaps the most significant single development since the original thesis was written is the global shift from passive regulatory frameworks—the kind the 2015 thesis criticized COPPA for representing—toward active, platform-level prohibitions on minor access.

Australia became the first country in the world to enact a nationwide social media ban for minors when the Online Safety Amendment (Social Media Minimum Age) Act 2024 took effect on December 10, 2025. The law prohibits children under 16 from holding accounts on designated social media platforms, including Instagram, TikTok, Facebook, Snapchat, and X. Platforms face fines of up to AUD $50 million (approximately USD $32 million) for systemic non-compliance. The Australian government is the first to answer the core criticism of this thesis—that passive legislation placing responsibility on end users is structurally insufficient—with a direct, platform-level mandate.

The Australian ban triggered immediate international attention. As of early 2026, France, the United Kingdom, Malaysia, Germany, Italy, Greece, and Spain were actively considering or advancing similar legislation. Whether these bans are ultimately effective is a live research question—civil liberties advocates and digital literacy researchers have raised concerns about unintended consequences—but their emergence represents a fundamental change in the global policy debate. The 2015 thesis's conclusion that "passive laws such as COPPA" are inadequate has been adopted as the working premise of a new generation of international legislation.

Within the United States, a parallel movement has targeted children's social media access in schools. As of early 2026, 28 or more states had enacted policies restricting cellphones or social media use in K-12 schools, with 22 of those enacted in 2025 alone. California's

Phone-Free Schools Act, signed in September 2024, mandates restrictions on student phone use statewide. Louisiana enacted a full school-day ban. North Carolina's legislation goes further, requiring instruction on social media's effects on mental health to be incorporated into school curricula. These policies represent a significant public policy acknowledgment that the harms documented in this thesis—psychological influence, distraction, and exposure to harmful content—are serious enough to warrant structural intervention in the educational environment.

The Social Media Landscape (2015–2026)

The social media landscape of 2026 is largely unrecognizable to the framers of the original 2015 thesis. Facebook, the central platform of that research, has seen its teen user base fall from approximately 71% to approximately 32% between 2014–15 and 2024–25 (Pew Research Center, 2024). The dominant platforms are now YouTube (90% of teens), TikTok (63%), Instagram (61%), and Snapchat (55%). AI-generated content, including deepfakes and synthetic media, has introduced new deception risks that were not contemplated in 2015.

TikTok, launched internationally in 2018, is characterized by an algorithm widely described as the most effective content recommendation engine ever deployed at consumer scale. Its ability to identify and exploit individual psychological vulnerabilities—including in minors—through algorithmically curated content has been the subject of extensive regulatory scrutiny, enforcement actions, and litigation.

Adolescent Mental Health & Social Media

The causal relationship between social media use and adolescent mental health—particularly for girls—has moved from contested theory to documented finding. The U.S. Surgeon General issued an advisory in 2023 explicitly warning about the mental health risks of social media for adolescents. Meta's own internal research (leaked in 2021) showed that Instagram made body image issues worse for approximately one in three teen girls. Pew Research Center (2025) found that 48% of teens say social media has a mostly negative effect on people their age, up from 32% in 2022. Adolescent depression

and anxiety rates have risen in parallel with smartphone and social media adoption curves.

Key Enforcement Actions & Litigation

Since 2015, social media companies have faced an escalating series of enforcement actions and class-action lawsuits. Notable cases include the FTC's 2023 complaint against Meta alleging COPPA violations; TikTok's $5 million FTC fine (2019) for COPPA violations; TikTok's $368 million EU fine (2023) for children's data mishandling; a $275 million Irish DPC fine against Meta (2022); and a 42-state Attorney General lawsuit against Meta (2023) for knowingly exposing minors to harmful content. These cases collectively represent a significant escalation in both enforcement severity and scope compared to the pre-2015 era described in this thesis.

Bibliography

The following bibliography preserves all original sources from the 2015 submission, followed by key 2016–2026 sources added in this updated edition.

Original Sources (2015)

Biometrics—It's all child's play! (2007, May). Biometric Technology Today, 7–8. doi:10.1016/S0969-4765(07)70120-0

Facebook forced into privacy business. (2010). Computer Fraud & Security, 2010(3), 1–2. doi:10.1016/S1361-3723(10)70015-4

Operators of online "virtual worlds" to pay $3 million to settle FTC charges. (2011, May 12). Retrieved from http://www.ftc.gov/news-events/press-releases/2011/05

The protection of children online: Risks faced by children online and policies to protect them. (2011). OECD Digital Economy Papers, 179, 105. doi:10.1787/20716826

The Social Habit, by Edison Research. (2012, July 22). Retrieved from http://www.slideshare.net/webby2001/the-social-habit-2012-by-edison-research

Google Spain SL v Agencia Española de Protección de Datos (AEPD), Case C-131/12 (Court of Justice of The European Union, May 13, 2014).

Preadolescence. (n.d.). (2014). In Merriam-Webster's online dictionary. Retrieved from http://www.merriam-webster.com/dictionary/preadolescence

Sony suffers major data breach as attackers leak files and destroy hard drives. (2014, December). Network Security, 2014(12), 1–2. doi:10.1016/S1353-4858(14)70116-3

Radio-frequency identification. (2015, April 28). Wikipedia, The Free Encyclopedia. Retrieved from http://en.wikipedia.org/w/index.php?title=Radio-frequency_identification

Anderson, J., & Ranie, L. (2012). Millennials will benefit and suffer due to their hyper-connected lives. Retrieved from http://www.pewinternet.org/2012/02/29/millenials-will-benefit-and-suffer-due-to-their-hyperconnected-lives/

Beals, B. (2002). Biometrics: hack proof? SANS Institute. Retrieved from http://www.giac.org/paper/gsec/2282/biometrics-hack-proof/103919

Brey, P. (2006). Evaluating the social and cultural implications of the Internet. Computers and Society, 36(3), 41–48.

Brown, D. H., & Pecora, N. (2014). Online data privacy as a children's media right: Toward global policy principles. Journal of Children and Media, 8(2), 201–207.

Buckingham, D. (2008). "Introducing identity." Youth, identity, and digital media. The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning, 1–24.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010, September). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548.

Fish, A., Li, X., McCarrick, K., Butler, S., Stanton, B., & Brumitt, G. (2008). Early childhood computer experience and cognitive development among urban low-income preschoolers. Journal of Educational Computing Research, 38(1), 97–113.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Philippines: Addison-Wesley Publishing Company.

FTC. (2015). The Internet of Things: Privacy & security in a connected world. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-Internet-things-privacy/150127iotrpt.pdf

Geddes, J. K. (2015). The secret life of kids online: What you need to know. Retrieved from http://www.parenting.com/article/kids-social-networking

Gillham, B. (2000). Case Study Research Methods. Bloomsbury Academic.

Glass, B., McGaw, B., & Smith, M. (1981). Meta-analysis in social research. Sage Publications.

Gray, S. (2007, September 25). Should schools fingerprint your kids? Retrieved from http://content.time.com/time/business/article/0,8599,1665119,00.html

Gutnick, A., Robb, M., Takeuchi, L., & Kotler, J. (2010). Always connected: The new digital media. New York: The Joan Ganz Cooney Center at Sesame Workshop.

Hillman, H., Hooper, C., & Choo, R. K.-K. (2014). Online child exploitation: Challenges and future research directions. Computer Law & Security Review, 30, 687–698.

Holloway, D., Green, L., & Livingston, S. (2013). Zero to eight: Young children and their Internet use. London, UK: EU Kids Online.

Jick, T. (1979). Mixing qualitative and quantitative methods: Triangulation in action. Administrative Science Quarterly, 602–611.

Johnson, G. M. (2010). Internet use and child development: Validation of the ecological techno-subsystem. Educational Technology & Society, 13(1), 176–185.

Kaufman, S. (2014, November 22). Alabama school system paid former FBI agent $157,000 to spy on black students: Critics. Retrieved from

http://www.rawstory.com/rs/2014/11/alabama-school-system-paid-former-fbi-agent-157000-to-spy-on-black-students-critics/

Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook. International Journal of Information Management, 34(6), 761–769.

Kumar, R. (2011). Research Methodology: A step-by-step guide for beginners (Third ed.). Thousand Oaks: Sage Publications.

Latimer, J., Dowden, C., & Muise, D. (2005). The effectiveness of restorative justice practices: A meta-analysis. The Prison Journal, 85(2), 127–144.

Lenhart, A., Purcell, K., Smith, A., & Zikcuhr, K. (2010). Social media and young adults. Pew Internet & American Life Project.

Logue, G. (2015). Pearson spying on student private social media accounts to determine if PARCC information is being leaked. Retrieved from http://missourieducationwatchdog.com

Mantelero, A. (2014, November 19). Finding a solution to the Google's dilemma on the "right to be forgotten." Retrieved from https://medium.com/@mantelero

McAfee. (2013, May 28). McAfee digital deception study 2013: Exploring the online disconnect between parents & pre-teens, teens and young adults. Retrieved from http://www.mcafee.com/us/resources/reports/rp-digital-deception-survey.pdf

McBride, D. (2011). Risks and benefits of social media for children and adolescents. Journal of Pediatric Nursing, 26(5), 498–499.

Messieh, N. (2012, April 18). Survey: 37% of your prospective employers are looking you up on Facebook. TNWNews.

Mohd, S. Y., Osman, N., Hassan, S. H., & Teimoury, M. (2014). Parents' influence on children's online usage. Procedia - Social and Behavioral Sciences, 155, 81–86.

Montgomery, K. C. (2014). Youth and surveillance in the Facebook era: Policy interventions and social implications. Telecommunications Policy, 38(9), 771–786.

Moren, D. (2014, December 30). 7 surprising biometric identification methods. Retrieved from http://www.popsci.com

Naeemi, S., Tamam, E., Hassan, S. H., & Bolong, J. (2014). Facebook usage and its association with psychological well-being among Malaysian adolescents. Procedia - Social and Behavioral Sciences, 155, 87–91.

Osborne, C. (2013, September 17). Apple iPhone fingerprint scanner raises security worries. ZDNet.

Pato, J. N., & Millett, I. L. (2010). Biometric recognition: Challenges and opportunities. Washington, D.C.: The National Academies Press.

Poulter, S. (2009, October 7). Children as young as five "using the Internet without parental supervision." Daily Mail.

Protalinski, E. (2012, April 13). 38% of kids on Facebook are under the minimum age of 13. ZDNet.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. Pew Research Center.

Ratan, D., Yuan, D., & Ross, K. W. (2013). Profiling high-school students with Facebook: How online privacy laws can actually increase minors' risk. 2013 Internet Measurement Conference, ACM.

Rosman, K. (2012, May 1). Tweens' secret lives online. Wall Street Journal.

Sauer, M. (2013). Data mining students through Common Core. The New American.

Saul, L. J., & Pulver, S. E. (1965). The concept of emotional maturity. Comprehensive Psychiatry, 6(1), 6–20.

Schwartz, M. (2010). The usage of Facebook as it relates to narcissism, self-esteem and loneliness. ETD Collection for Pace University.

Simpson, M. (2014). Social networking nightmares: Cyberspeak no evil. NEA. Retrieved from http://www.nea.org/home/38324.htm

Stinson, J. (2014, October 27). States backtrack on student tracking technology. Pew Trusts Stateline.

Taneja, A., Vitrano, J., & Gengo, N. (2014). Rationality-based beliefs affecting individual's attitude and intention to use privacy controls on Facebook. Computers in Human Behavior, 38, 159–173.

Tynan, D. (2014, November 13). What scares parents most about tech? Yahoo Tech.

Zwerdling, D. (2013, September 30). Your digital trail, and how it can be used against you. NPR.

Updated & Added Sources (2016–2026)

American Psychological Association. (2023). Health advisory on social media use in adolescence. Retrieved from https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.pdf

CareerBuilder. (2023). Annual social media recruitment survey. Retrieved from https://www.careerbuilder.com

Federal Trade Commission. (2025). Amendments to the Children's Online Privacy Protection Rule. Federal Register, 90(77). Retrieved from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Kemp, S. (2024). Digital 2024 Global Overview Report. We Are Social & Meltwater.

Murthy, V. H. (2023, May 23). Social media and youth mental health: The U.S. Surgeon General's advisory. Retrieved from https://www.hhs.gov/surgeongeneral/reports-and-publications/social-media-advisory

Pew Research Center. (2024, December 12). Teens, social media and technology 2024. Retrieved from https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/

Pew Research Center. (2025, April 22). Social media and teens' mental health: What teens and their parents say. Retrieved from https://www.pewresearch.org/internet/2025/04/22/teens-social-media-and-mental-health/

Rideout, V., Peebles, A., Mann, S., & Robb, M. B. (2022). Common Sense Census: Media use by tweens and teens. Common Sense Media.

Wall Street Journal. (2021, September 14). Facebook knows Instagram is toxic for teen girls, company documents show. Wall Street Journal. Retrieved from https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.

Australian Government. (2024). Online Safety Amendment (Social Media Minimum Age) Act 2024. Canberra: Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

Federal Bureau of Investigation. (2023). Sextortion: A growing threat preying upon our nation's teens. Washington, D.C.: FBI. Retrieved from https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens

Internet Crime Complaint Center (IC3). (2024). Child sexual abuse material created by generative AI and similar online tools is illegal. FBI. Retrieved from https://www.ic3.gov/PSA/2024/PSA240329

National Center for Missing and Exploited Children (NCMEC). (2025). CyberTipline 2025 interim report. Alexandria, VA: NCMEC.

Thorn. (2025). The state of sextortion in 2025: Annual research summary. Thorn Digital Defenders. Retrieved from https://www.thorn.org/blog/the-state-of-sextortion-in-2025/

United States Congress. (2025). Eliminating Nonconsensual Online Lewd and Exploitation Concerning Everyone (ENFORCE) Act, S. _____, 119th Cong. (2025). Passed U.S. Senate December 2025.

United States Congress. (2025). Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks (TAKE IT DOWN) Act, Pub. L. No. 119-___. Signed by President Trump, May 2025.

United States Congress. (2024). Kids Online Safety and Privacy Act (KOSPA), S. 2073, 118th Cong. Passed U.S. Senate 91–3, July 2024.

Garcia King, M., & Lim, J. (2024, October 23). The teens and young adults suing Character.AI over suicides, self-harm and sexual content. NBC News. Retrieved from https://www.nbcnews.com/tech/internet/character-ai-chatbot-lawsuits-teens-suicide-self-harm-sexual-content

ExcelinEd. (2026, January 21). Top 2025 policy trend: 28 states commit to phone-free classrooms and schools. ExcelinEd in Action. Retrieved from https://excelinedinaction.org/2026/01/21/top-2025-policy-trend-28-states-commit-to-phone-free-classrooms-and-schools/

Federal Trade Commission. (2023, May 3). FTC proposes blanket prohibition preventing Facebook from monetizing youth data. FTC Press Release. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-blanket-prohibition-preventing-facebook-monetizing-youth-data