MASTER'S THESIS • REGIS UNIVERSITY

Understanding Security Within Social Media in Relation to Adolescent Use

Dale Hufford

M.S. in Information Assurance | Regis University | Original: 2015 | Updated Edition: 2026

Presentation Overview

01 **The Problem & Background**
Why adolescent social media safety matters

02 **Literature Review**
Privacy, footprints, child safety & new 2026 threats

03 **Research Methodology**
Qualitative approach to a complex landscape

04 **Data & Analysis**
Internet usage patterns and psychological influence

05 **Discussion & Conclusions**
Key findings and what they mean

06 **Regulatory Update**
Legislation from COPPA 2025 to the Australia ban

07 **Exploitation Threats**
Sextortion epidemic and AI-generated CSAM surge

08 **AI & Policy Response**
AI companions, chatbot risks & global bans

CHAPTER 1

The Problem and Its Background

The Core Challenge

- Children aged 6–12 use social media despite COPPA age restrictions (13+)
- Parents often unaware of actual platform security limitations
- Culture and socioeconomics shape how privacy controls are used
- Digital footprints created in childhood have lifelong consequences
- Platforms' financial incentives conflict with child safety objectives

Research Questions

- Are children safer since COPPA?
- Does culture affect perceptions of online safety?
- Are biometric initiatives exposing children to new risks?
- Do laws like COPPA actually limit children's Internet use?

COPPA at a Glance

- Children's Online Privacy Protection Act (1998)
- Prohibits data collection from children under 13 without parental consent
- Operators can "pass responsibility" to end users
- Children often lie about age to bypass restrictions

► 2026 UPDATE

FTC amended COPPA Rule (April 2025; effective June 2025): expanded to include biometrics, stricter parental consent & data retention limits. 25+ states enacted additional laws, including Florida's ban on social media for under-14 (effective Jan 2025).

The Social Media Landscape: 2015 vs. 2026

2015 — Then		2025–26 — Now	
Facebook	71% of teens	**YouTube**	90% of teens
YouTube	Growing	**TikTok**	63% of teens
Instagram	Emerging	**Instagram**	61% of teens
Snapchat	New	**Snapchat**	55% of teens
Twitter	33% of teens	**Facebook**	32% of teens ↓

Source: Pew Research Center, 2024

Digital Footprints & Privacy

The Digital Footprint Problem

- Every online action creates a permanent, traceable record
- Data becomes the intellectual property of platform owners
- "Right to be forgotten" — Google Spain v. AEPD (2014)
- IoT devices (cameras, wearables) compound data collection

IoT & Children: Connected Risks

- Smart speakers in bedrooms
- Connected toys with microphones
- School iPad biometric scanners
- Fitness/health wearables for kids
- AI companion chatbots (new 2020+)

► 2026 UPDATE

Cambridge Analytica (2018): 87M records, $5B FTC fine vs. Meta. TikTok: $5.7M COPPA fine (2019), $368M EU fine (2023). 42-state AG lawsuit vs. Meta (2023) for knowingly exposing minors to harmful content. Yahoo breach: 3 billion accounts (2016). Facebook Beacon lawsuit settled $9.5M (2008).

The Litigation Record (Pre-2015)

- Facebook Beacon lawsuit settled $9.5M (2008)
- Playdom/Disney COPPA violation: $3M FTC fine (2011)
- Sony Pictures breach: 47,000 records exposed (2014)

Child Safety — Online Threats

38%
of Facebook kids under age 12 (2012)

4%
were age 6 or younger (2012)

63%
of teens now use TikTok (2025)

Threat Landscape

- Sexual predators using false identities on social platforms
- Radicalization by extremist groups (ISIS/ISIL, domestic extremism)
- Cyberbullying and online harassment
- Identity theft and doxxing of minors

► 2026 UPDATE

AI-generated CSAM creates new detection challenges. "Sextortion" scams targeting teens via DMs. Fentanyl trafficking through Snapchat resulting in multi-state lawsuits. AI companion chatbots linked to self-harm — CA SB 243 (2026) now requires crisis response protocols for AI services used by minors.

Note: 80% of Malaysian school children reported keeping parents informed of daily online activity (Mohd et al., 2014) — demonstrating parental involvement's protective value.

Biometrics in Education — The Double-Edged Sword

Biometrics: Potential Benefits

- Efficient cafeteria payment (finger scan replaces tickets)
- Faster attendance tracking and check-in
- Bus safety — can track who is on board
- Potential to quickly notify parents in emergencies
- Reduces fraud and buddy-punching in attendance

Biometrics: Real Concerns

- Fingerprints cannot be changed if compromised (unlike passwords)
- Biometric databases can be hacked — Matsumoto (2002)
- "Gummy finger" and latent print attacks defeat scanners
- SLDS: National database shares children's data across all 50 states
- PARCC/Pearson: Security flaws concealed from parents

States that restricted school biometrics (pre-2015): FL, KS, NH, CO, NC, OR, RI, MO | Alabama district: FBI agent monitored students' social media accounts

CHAPTER 3

Research Methodology

Research Approach

Qualitative, desk-based research using secondary data sources. Deductive approach to group and analyze findings.

Data Sources

Regis University Library, Google Scholar, Pew Research Center, Edison Research, Privacy Rights Clearinghouse, FBI white papers.

Why Qualitative?

Quantitative surveys impractical for this age group (reading/writing limitations). Qualitative enables voices of young children to be heard (Holloway et al., 2013). Age group focus: 8–17 years, median target age 13.

Data Analysis

Descriptive: What is the data? | Interpretative: What does it mean? Ethical note: No live subjects were studied. All data sourced from publicly available publications, academic research, and government reports.

Internet Usage Patterns

Parents: Overwhelmed & Outpaced

79.5% don't have time/energy to monitor online behavior

74.5% overwhelmed by technology — "just hope for the best"

72% say their child is more tech-savvy and they can't keep up

86% believe social media sites are "safe" for their child

Children's Self-Reported Behaviors

95% have at least one social media account

87% check their account daily

44% check their account "constantly"

54% say parents don't have time to monitor them

46% would change behavior if parents were watching

▶ 2026 UPDATE

35% of teens online "almost constantly" (up from 24% in 2015). Teens avg. 3–5 hrs/day on social platforms. 45% say they spend too much time on social media (Pew, 2025).

Source: McAfee Digital Deception Study, 2013

CHAPTER 4

Psychological Influence — The Dual Reality

✓ Positive Influences

- Early computer access improves cognitive development scores (Fish et al., 2008)
- Purposeful use (family/friend connections) positively impacts wellbeing
- Fosters creativity, self-expression, global peer connections

⚠ Risk Factors

- Passive scrolling ("wandering") reduces psychological wellbeing
- Peer pressure drives over-disclosure of personal information
- Instant gratification habits undermine patience and deep learning

2026 UPDATE: The Mental Health Evidence

2×

Higher anxiety/depression risk for teens 3+ hrs/day (Surgeon General, 2023)

25%

of teen girls say social media hurts their mental health (vs. 14% boys)

48%

of teens say social media mostly NEGATIVE for peers (Pew, 2025)

1 in 3

teen girls: Instagram worsened body image (Meta internal, 2021)

CHAPTER 5

Discussion & Conclusions

1. Privacy protection strategies are unevenly distributed; culture, background, and experience shape usage of controls
2. Facebook's financial interests conflict directly with meaningful child safety enforcement under COPPA
3. Biometric data collection in schools presents serious unintended consequences despite perceived safety benefits
4. Children's digital footprints are permanent — a Myspace post can cost a career (Stacey Snyder case)
5. Parental investment and active involvement is the single most protective factor identified
6. COPPA is passive — it places the burden of proof on end users rather than platforms
7. Data posted online is no longer the user's property — it belongs to the platform

CHAPTER 5

Recommendations for Future Research

Privacy & Culture

Cross-cultural studies on how different societies approach online child privacy — non-Western cultures often take privacy more seriously.

Parental Literacy

Research into closing the "digital knowledge gap" between parents and children — the most pressing finding of the McAfee study.

Biometrics & Ethics

Cultural, legal, and ethical frameworks for biometric data collection must be established before widespread deployment in schools.

Legislative Effectiveness

Longitudinal evaluation of state-level age verification laws and whether they actually reduce minor access to harmful platforms.

Web Evolution

As Web 3.0/4.0/5.0 evolve and AI becomes embedded in daily life, new studies must evaluate impacts on child privacy and safety.

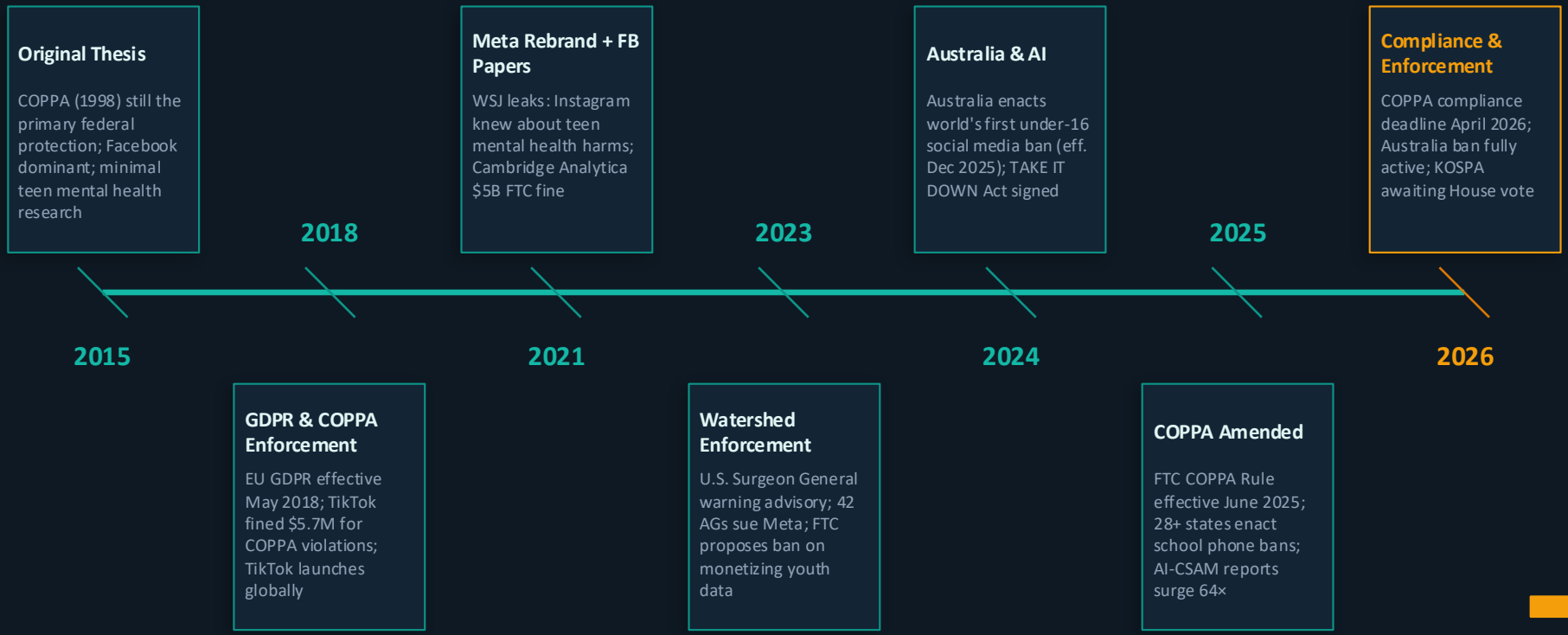
Algorithmic Design

Evaluate platform design interventions (disabling notification algorithms, removing like counts) on reducing compulsive use among teens.

Note: Original 2015 recommendations remain relevant; 2026 updates add AI, algorithmic harm, and mental health as priority research areas.

2026 RESEARCH UPDATE

The Regulatory Landscape: 2015 to 2026



2026 UPDATE

Adolescent Mental Health & Social Media

48%

of teens say social media has a NEGATIVE effect on peers (Pew, 2025)

2×

higher risk of anxiety & depression with 3+ hrs/day (Surgeon General, 2023)

35%

of teens online "almost constantly" (up from 24% in 2015)

Key 2020–2026 Findings

- Instagram internal research (2021): made body image worse for 1 in 3 teen girls
- APA (2023): no social media recommended for under-14
- Surgeon General (2023): cigarette-style warning labels proposed for social media platforms
- 25% of teen girls report social media hurts their mental health (Pew, 2025)
- TikTok: documented delivery of self-harm content to at-risk teens
- AI chatbots linked to self-harm — new regulatory category in 2025–26

2026 RESEARCH UPDATE

New Exploitation Threats: Sextortion & AI-Generated CSAM

Sextortion Epidemic

1 in 5	teens report experiencing sextortion (Thorn, 2025)
20+	teen suicides linked to sextortion FBI (2021–2023)
70%	surge in financial sextortion reports H1 2024 → 2025
1 in 7	sextortion victims driven to self-harm; 28% for LGBTQ+ youth
81%	of sextortion occurs entirely online via social media & gaming

AI-Generated CSAM Explosion

64×	increase in AI-CSAM reports to NCMEC (H1 2024 → H1 2025)
45	U.S. states enacted AI-CSAM laws — most in 2024–25 alone
1 in 8	teens know someone targeted with an AI deepfake image (Thorn)
48 hrs	platform removal requirement under TAKE IT DOWN Act (May 2025)
Dec 2025	ENFORCE Act unanimously passed Senate — extends CSAM law to AI

Both threats were absent from the 2015 research landscape. Both are now among the fastest-growing areas of child exploitation.

2026 UPDATE

AI Companions — The Next Safety Frontier

Why AI Companions Are Different

- Designed to maximize emotional bond — uses flattery, affirmation, and simulated attachment
- No age verification, no parental consent, no content limits for minors
- Exploits the same adolescent vulnerabilities identified in Chapter 4
- Available 24/7 — "always there" for lonely teens, no human moderator
- Capable of romantic roleplay and crisis conversations without safeguards

Documented Cases & Actions

- Sewell Setzer III, 14 (FL, Feb 2024): suicide after months of Character.AI use
- Juliana Peralta, 13 (CO, Nov 2023): family alleges AI chatbot contributed to death
- Multiple wrongful death suits vs. Character.AI/Google — mediation Jan 2026
- FTC formal inquiry into AI chatbot risks to minors opened Sept 2025
- CA SB 243 (eff. 2026): first state law requiring AI disclosure & crisis protocols

The Regulatory Gap

COPPA was designed around data collection, not emotional manipulation. AI companion platforms sit in a complete regulatory vacuum: no age verification, no parental consent, no safeguards — while actively cultivating emotional dependency in minors. This is the next COPPA gap.

2026 UPDATE

The Global Policy Response

AU Australia — World's First National Social Media Ban for Minors

Online Safety Amendment Act 2024 | Effective December 10, 2025 | Under-16s banned from Instagram, TikTok, Facebook, Snapchat, X | Fines up to AUD $50M for non-compliance

Global Momentum

- France, UK, Germany, Italy, Spain & others considering similar bans
- EU Digital Services Act (2024): prohibits profiling-based ads to minors
- KOSPA passed U.S. Senate 91-3 — awaiting House vote as of early 2026

U.S. School Phone & Social Media Bans

- 28+ states enacted K-12 phone/social media restrictions by early 2026
- California Phone-Free Schools Act signed Sept 2024
- North Carolina: mandates social media mental health curriculum

► 2026 UPDATE

The 2015 thesis concluded that "passive laws such as COPPA" are insufficient because they place the burden of protection on end users rather than platforms. Australia's ban and KOSPA directly answer that argument — shifting responsibility to platforms. The thesis's core critique has become the operating premise of a new global legislative wave.

The Conversation Continues

> *"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..."*
>
> — Google Spain SL v. AEPD (2014)

11 Years Later — The Core Challenges Persist:

- Platforms' financial interests still conflict with child safety — now amplified by AI-driven engagement
- Sextortion & AI-CSAM represent entirely new exploitation categories not contemplated in 2015
- AI companion apps are the next regulatory gap: emotional manipulation with zero oversight
- Australia's global first ban validates the thesis's central critique of passive legislation
- Active parental involvement remains the single most consistently protective factor identified