Youth Digital Safety and Gender-Based Violence

Exploring a digital safety ecosystem through multi-stakeholder perspectives

March 13, 2026

Sociotechnical Systems and Wellbeing Research Lab (SWRL)
Brown University, Department of Computer Science

This research project was funded and conducted in collaboration with the New York State Office for the Prevention of Domestic Violence, Bureau of Law Enforcement and Public Safety, through a 2024 State of the State Initiative by New York State Governor Kathy Hochul

Diana Freed, Alyssa Lanter, Maya De Los Santos, Daniel Schiffman, Daniel Sedarous, Alexandra Hogue, Sophia Lloyd George, Jackson Schwartz, Ethan McDowell, Papayaw Afari, Shadrack Annor, Rachel Brooks, Kosta Karathanasopoulos, Christie Cadet

Background 1
Executive Summary 1
The Digital Landscape Facing Youth 2
Critical Themes 3
Looking Ahead 3
Introduction 3
Methodology 4
Demographics 5
Youth 6
Key Findings 6
How Youth Trust Others Online 7
Stories of Deception 7
Trust and Gaming 8
The Gaming Exploitation Pipeline 8
Education on Digital Safety is Not Enough 9
Location Sharing 9
Bypassing Parental Controls 10
Technological Considerations for Special Populations 10
Parents 11
Key Findings 11
Parental Protective Practices 11
Youth Workarounds 11
Technology Use Through Lived Trauma 12
Perspectives of Social Media 12
Gaming 12
Parents' Protective Practices 13
AI and Synthetic Media as Emerging Threats 13
Sextortion and Coercion 13
Educators 14
Key Findings 14
Youth Monitoring 14
Barriers Educators Face 14
Tensions Between Educators and Parents 14
Educator Training Needs 14
Influences on Youth's Behaviors 15
Youth Digital Safety Education 15
Monitoring of Youth 16
Harms Toward Youth Identified By Educators 16
Barriers to Schools' Response to Harm 17
Knowledge Gaps Identified by Educators 17
Law Enforcement 18
Key Findings 18
Distinct Social Groups Correlate with Different Levels of Threats 19
The Broader Pattern: Cycles of Victimization 20
Tech-Facilitated Harms and Peer-to-Peer Sextortion 20
Adult Misconceptions and Discomfort with Digital Harms 21
Key Stories 22
Online Sexual Exploitation and Abuse of Youth Using Technology 22

Online Sexual Exploitation and Abuse of Girls Using Technology 22
Online Sexual Exploitation and Abuse of Boys Using Technology 23
Online Sexual Exploitation and Abuse of LGBTQ Youth Using Technology 23
Teen Interpersonal Violence 24
Conclusion 24
References 26
Definitions 27, 28

Note to readers: This paper contains descriptions of coercion, sextortion, non-consensual image sharing, deepfakes, sexual exploitation, and interpersonal violence against youth.

Background

To combat the growing and evolving problem of technology-facilitated gender-based violence against teens, Governor Hochul introduced the Safeguard Teens from Online Sexual Exploitation Initiative in her 2024 State of the State proposal. Through this action, Governor Hochul tasked the Office for the Prevention of Domestic Violence (OPDV) with educating the public on technology-facilitated gender-based violence (TFGBV), the misuse or manipulation of technology to commit any harmful threat or act directed at an individual or group based on actual or perceived sex, gender, gender identity, sex characteristics, or sexual orientation, sextortion, deepfakes, and the evolving role artificial intelligence (AI) plays in gender-based violence in order to safeguard the youth of New York State (NYS) through public awareness, training and technical assistance, and the creation of a TFGBV public-facing website.

The OPDV, created in 1992, is the country's only cabinet-level executive state agency dedicated to the issue of gender-based violence. It replaced the former Governor's Commission on Domestic Violence established in 1983. OPDV's mission is to improve the state's response to and prevention of domestic violence with a goal of enhancing the safety of all New Yorkers in their intimate and family relationships. OPDV has a vision to create a state in which communities and systems are committed to supporting and promoting equality, dignity, and respect so that individuals can feel safer in their relationships.

Under the law that created the agency, OPDV's role is to advise the Governor and the Legislature on policies and best practices, train professionals across the state, and serve as a resource on the issue of domestic violence. Executive Law § 575 states that OPDV shall advise the Governor and the Legislature on the most effective ways for the state government to respond to the problem of domestic violence. In fulfilling this responsibility, the office shall consult with experts, service providers, and representative organizations in the field of domestic violence and shall act as an advocate for domestic violence victims and programs. OPDV shall also develop and implement policies and programs designed to assist victims of domestic violence and their families, and to provide education and prevention, training and technical assistance.

For the past several decades, New York State has worked to protect survivors through public policy, education, and programming. From the establishment of the first domestic violence shelter in NY, to the development of the new text and chat feature of the Domestic Violence and Sexual Violence Hotline, OPDV has evolved to meet the needs of survivors of domestic violence, sexual assault, and gender-based violence. OPDV believes that survivors of all forms of gender-based violence deserve support that is survivor-centered, trauma-informed, and culturally responsive.

In order to ensure that this work is informed by the real experiences of youth and other stakeholders in New York State, OPDV partnered with Dr. Diana Freed of Brown University to conduct a study into this growing topic for this report. Dr. Freed is an Assistant Professor of Computer Science and Data Science at Brown University, where she is the Director of the Sociotechnical Systems and Wellbeing Research Lab (SWRL). Her research focuses on designing, developing, and evaluating systems in the context of youth interpersonal relationships, intimate partner violence, and caregiving systems. She is also a Faculty Associate at the Harvard Berkman Klein Center for Internet and Society. Dr. Freed co-founded the Youth Leadership Advisory Board (YLAB), an initiative that engages with high school students to examine the pressing social challenges adolescents encounter in digital environments with a focus on socially responsible computing and AI literacy.

Executive Summary

In partnership with the Office for the Prevention of Domestic Violence (OPDV), the research team conducted a statewide study with youth, educators, parents, and law enforcement to gain insight into the way teens use technology and how it impacts gender-based violence, the risks they may face online, and

how to best protect youth and respond to these risks. In the study, we heard from 76 New Yorkers from across the state: 14 law enforcement professionals, 15 parents, 24 educators, and 23 youth. We conducted semi-structured interviews and focus groups via a video conferencing platform. We conducted this study in an interview format to ensure that future work would be grounded in the real experiences of New Yorkers impacted by this issue. This report serves as a foundational guide with insights that will inform future research, policies and training materials on youth digital safety for stakeholders and the public on this important issue.

The Digital Landscape Facing Youth

Youth navigate an interconnected web of platforms — social media platforms like Snapchat, Instagram, TikTok, YouTube, Discord, and online gaming environments like Roblox and Fortnite — where their social, educational, and emotional lives unfold simultaneously. While parents, schools, and governments have invested in safety tools such as parental-control apps, classroom monitoring systems, and digital literacy curricula, concerns about youth exposure to online harm continue to rise. The threats youth face include sextortion, impersonation, catfishing, non-consensual intimate image sharing, AI-generated deepfakes, grooming by predators and peers, cyberbullying, financial exploitation, and teen dating violence facilitated through technology.

Youth reported that trust online is relational, not technical. This means they determine who to trust and interact with based on mutual friends and shared connections or interests (e.g., same or nearby school mentioned in a profile bio, similar taste in music mentioned, etc.), rather than platform safety features. Malintentioned perpetrators are able to take advantage of this by creating accounts pretending to be trustworthy to youth in order to gain their trust. Youth demonstrated high digital literacy, but described the need for institutional safety education to be consistently updated to align with the threats they may experience due to issues that include AI deepfakes, extortion, and sextortion. Notably, half of surveyed teens admitted to bypassing parental or school digital controls, not out of defiance, but because those controls felt misaligned from their real-world needs. Youth expressed that they wanted agency, transparent systems, practical guidance, and shared accountability rather than unilateral surveillance.

Parents described managing digital risk as a form of crisis response rather than everyday parenting. Many parents had opinions of platforms that did not align with the actual risks of those platforms. For example, parents perceive gaming platforms as safe while remaining unaware of in-game communication channels that expose children to strangers and predators. Parents expressed frustration with the limitations of parental-control tools, which were often costly, confusing, or easily bypassed. Several parents had direct experience with sextortion incidents involving their children and described reporting mechanisms and law enforcement response as compliant but ultimately unable to address the harm.

Educators reported feeling overwhelmed by the responsibility placed on schools to protect students from digital harms while lacking adequate time, training, and resources. They described monitoring students through both digital alerts and physical observation but noted significant legal barriers limiting how schools can respond to reports of online harm. Educators identified loneliness as a key driver of risky online behavior among students and called for parents to take a more active role. They also flagged that youth routinely bypass school-level digital restrictions and that current digital literacy education does not address emerging threats like deepfakes and AI-facilitated harms.

Law enforcement professionals described an environment in which vulnerable youth, many with behavioral or developmental challenges, face growing exposure to digital and interpersonal harms. Officers reported that they frequently occupy hybrid roles combining enforcement, counseling, and mediation. They identified a troubling normalization of harmful behaviors among youth, including the casual creation and distribution of intimate images and a lack of understanding of what constitutes stalking or unhealthy relationship dynamics. Law enforcement reported rising cases of peer-to-peer sextortion, including elaborate schemes involving peers in the same school, as well as technology-facilitated violence that manifests on social media. They emphasized that many young people do not recognize themselves as victims until years after

patterns of abuse began.

Critical Themes

Several overall themes emerged from this research. First, **gaming platforms have become documented avenues for exploitation**. The research identified a three-stage gaming exploitation pipeline: initial contact through in-game chat, migration to perceived private platforms like Discord or Snapchat, and exploitation through sextortion and coercion. Parents were often unaware of the risks embedded in gaming environments or the communication channels they enable.

Additionally, **AI and synthetic media represent rapidly emerging threats**. Parents and law enforcement described incidents involving AI-generated deepfakes used for sextortion, youth relying on AI chatbots as substitutes for mental health professionals, and voice synthesis technology that raises the possibility of impersonation attacks.

Stakeholders noted that **gender-based violence manifests in digital environments in distinct and escalating ways**. In this study we found that youth of all gender identities experienced targeted grooming, sextortion, and non-consensual image creation and distribution. We also found that males were disproportionately victimized in peer-to-peer sextortion schemes, often through gaming platforms and social media. LGBTQ youth are particularly vulnerable to manipulation by predators who exploit their need for community and acceptance. Additionally, teen dating violence is amplified through technology, as constant digital contact may normalize controlling and coercive behaviors.

Looking Ahead

This report reveals a persistent gap between institutional models of safety and the lived realities of young people navigating complex digital environments. Closing this gap will require coordinated, multi-stakeholder action: updated and responsive digital literacy education in schools, stronger and more usable platform-level protections, better-resourced law enforcement capacity for technology-facilitated crimes, and support for parents, guardians, and caregivers who are currently navigating the complexity of youth digital safety. OPDV will use the findings in this report to close this gap by informing future policies, trainings, and public resources aimed at protecting New York's youth from technology-facilitated gender-based violence.

Introduction

Youth operate in digital environments that are more expansive, interconnected, and surveilled than at any previous moment in history. Their social, educational, and emotional lives unfold across many platforms, each designed to maximize connection while quietly embedding mechanisms of data extraction, behavioral tracking, and algorithmic curation. At the same time, parents, schools, and governments have invested heavily in new safety infrastructures: parental-control apps, location tracking apps, school-issued device monitoring systems, awareness programs, and digital citizenship programs. Yet despite this growth of protective technologies, concerns about youth exposure to online harm, including sextortion, extortion, impersonation scams, non-consensual image sharing, and AI-generated deepfakes, continue to rise.

With the prevalence of smartphones and widespread use of social media and communication platforms, there are increasingly more opportunities for dangerous interactions in online spaces, particularly for youth. In the current climate, youth face varying levels of digital harms such as cyberbullying, sexual violence, financial fraud, and misinformation in online spaces [1]. Prior work has shown that within these environments, perpetrators may move interactions with youth from one platform to another, sometimes even transitioning into the physical world [1]. As technology becomes more sophisticated, the landscape of digital harms, particularly with extortion and sextortion, is changing as well.

Extortion and sextortion are prevalent threats that youth may face when interacting with perpetrators online, causing mental and emotional distress, with the population aged 13-17 being the most vulnerable [2]. Extortion and sextortion cause extreme stress and pressure on victims, creating situations of duress when trying to process and handle these threats. The FBI also published that there has been an increase in cases of extortion involving children, making this a significant area of interest for threat mitigation [3]. Additionally, there has been a reported rise in sextortion amongst youth (typically within the ages of 14-17) within the context of financial scams, where a perpetrator asks for intimate photos in order to extort money from the victim [4]. Perpetrators may employ different methods and instigate different levels of harm against youth in this space in order to successfully extort targets, making it vital to learn how to effectively mitigate technology-facilitated threats.

Victims are more likely to under-report incidents of sextortion and extortion due to shame [5, 6]. This creates challenges for victims seeking out support networks and proper resources to handle harms, negatively impacting help-seeking behaviors. In prior work, Freed et. al [7] has found that youth will overwhelmingly cope with technology-facilitated gender-based violence, including sextortion and extortion, on their own. Therefore, it is vital to understand what perceptions stakeholders within a youth's support network, such as parents and educators, have around these issues and what measures can be taken to prevent and reduce cases of sextortion and extortion.

In this report, through findings from semi-structured interviews and focus groups, we examine how youth conceptualize and act on digital safety in their everyday lives. We also include the experiences of educators, parents, and law enforcement that provide support to youth. Our data reveals that safety is not experienced as a static state or a simple adherence to rules but as a process of continuous change that involves deciding who to trust, what to share, when to comply, and when to resist. Youth participants described relying on relationship-based cues, including mutual friends, shared group membership, or recognizable offline ties, to authenticate identity online; they navigated family governance structures that blurred care with control; and they encountered school surveillance systems that framed safety as compliance, prompting creative workarounds. They also faced new forms of harm, including AI-assisted sextortion and image manipulation, while simultaneously integrating generative AI tools into everyday learning and emotional support. Across these diverse practices, adolescents framed safety as competence: the ability to recognize, respond to, and recover from risk rather than to avoid it entirely.

Our analysis contributes insights that inform ongoing debates about youth digital-safety. First, we demonstrate that youth safety strategies are relationally organized — embedded in the social fabric of peers, families, and institutions rather than in isolated acts of individual caution. We show that current safety infrastructures often function less as protective technologies than as areas of negotiation, where authority, trust, and autonomy are constantly recalibrated. Additionally, our analysis shows how perpetrators and adversaries exploit the features of digital systems and generative AI to weaponize social engineering, leveraging identity ambiguity and automation to scale coercion.

Methodology

To develop a comprehensive understanding of the risks youth face in the digital world, particularly around sextortion and related extortion, we conducted a qualitative study that involved semi-structured interviews and focus groups with 76 participants. We sought to gain insights into how relevant stakeholder groups perceive and respond to gender-based violence in the digital world. All study participants were recruited by the Office for the Prevention of Domestic Violence (OPDV) through distributed flyers, targeted email outreach, and public announcements.

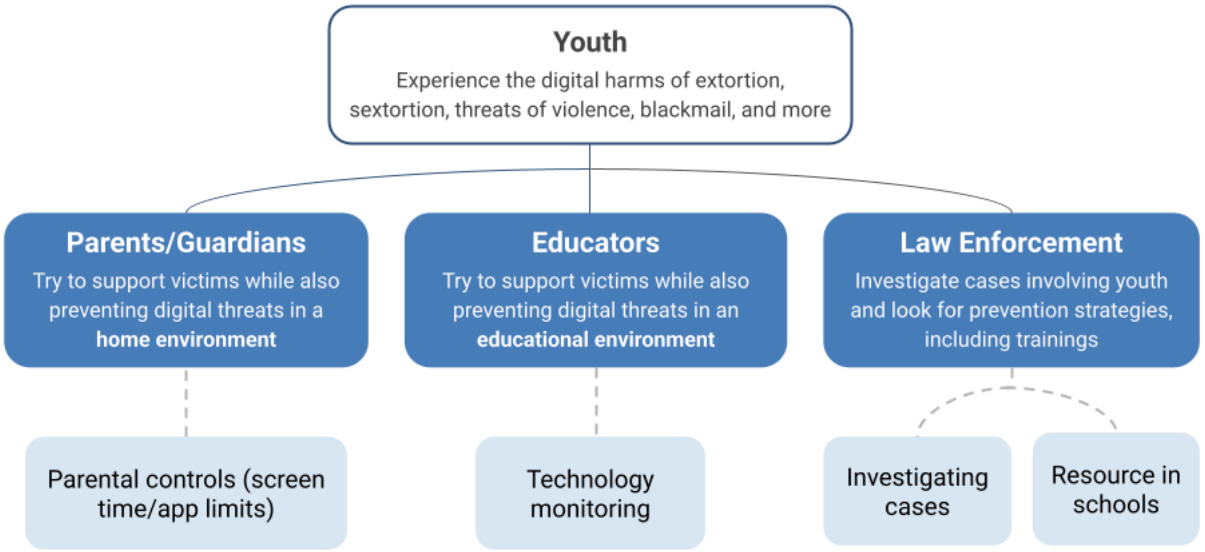
In the study, we heard from 14 law-enforcement professionals, 15 parents, 24 educators, and 23 youth. We conducted semi-structured interviews and focus groups via a video conferencing platform with the additional option for youth to opt for a long form survey, instead of a live focus group. All data collection

took place between June and October 2025. Interviews and focus groups lasted 60-90 minutes and were audio-recorded and transcribed for analysis.

Each session began with a review of study procedures and an opportunity to ask questions before providing consent. All sessions followed a discussion guide focused on topics that included identifying, understanding, and mitigating online harms. Basic demographic information was collected through the recruitment questionnaire used to screen participants. Participants, excluding law enforcement, were invited to complete an optional pre-interview survey to capture their online-safety practices and familiarity with digital-risk topics and to provide additional context for interpreting the interview data. Completion of the pre-survey was voluntary and not required for participation. In total, 15 parents, 18 educators, and 9 youth completed the pre-interview survey.

The study protocol was approved by Brown University's Institutional Review Board (IRB) and complied with all ethical guidelines for human-subjects research. Parental permission and youth assent were obtained for all participants under 18 years old. All participants were reminded that their involvement was voluntary and that they could withdraw at any time without penalty.

In the following sections we discuss the results for each stakeholder group.



Demographics

This study included 76 participants comprised of 23 youth and 53 adults. The adult participants ranged in age from 22 to 62, with 2 individuals not reporting age. Of the adult participants, 40 participants identified as female (75.5%) and 13 as male (24.5%). Among the 47 adult participants who reported race and ethnicity, 30 identified as White (63.8%), 10 as Black (21.3%), 3 as Asian (6.4%), 2 as Hispanic (4.3%), 1 as Mixed (2.1%), and 1 as White Hispanic (2.1%).

The youth participants ranged in age from 13 to 20; 4 did not report complete demographic information. Of the total youth sample, 12 identified as female (52.2%) and 11 identified as male (47.8%). Among the 19 youth participants that reported race and ethnicity, 10 identified as White (52.6%), 4 as Black (21%), 3 as Asian (15.8%), 1 as Mixed (5.3%), and 1 as White Hispanic (5.3%).

Geographically, participants were distributed across urban, suburban, and rural or small-town communities. Eighteen participants resided in urban areas (34.0%), 23 in suburban communities (43.4%), and 10 in rural or small-town locations (18.9%); 2 participants did not indicate location (3.8%). Overall, the sample reflects demographic and geographic diversity, supporting analyses attentive to variation in gender, race/ethnicity, and community context.

Data protection: All participants were offered the option to participate anonymously; two youth elected to do

so. To further protect participants, we do not disclose the names of partner organizations, schools, or agencies that assisted in recruiting participants and have removed identifying information about participants and any individuals they referenced from all session recordings and transcripts. When reporting our findings, we omit unique details, phrases, or words from quotes to mitigate identification.

Youth

23 unique youth participants, ages 13–20 took part in the study.

Key Findings

- Trust is relational, not technical, mutual friends and known networks guide perceived safety.
- Youth stated that AI is deeply embedded in academic life in which youth use Snapchat AI for homework and ask advice from ChatGPT.
- Snapchat's built-in AI acts as a ubiquitous peer presence for advice seeking and homework help.
- Sextortion, impersonation, and AI-enabled image manipulation are rising harms, underaddressed by current curricula.
- Institutional education — through school assemblies or "digital citizenship" lessons — feels dated, vague, and unresponsive to emerging threats.
- Schools utilize web filtering and monitoring software, Wi-Fi restrictions, and device monitoring systems, yet youth routinely find ways to work around these restrictive measures
- Families often use screen-time monitoring tools, but several youth reported easily bypassing these restrictions, often by device recording their parents entering the screen-time password.
- Youth seek co-agency — they want transparent systems, practical guidance, and shared accountability rather than unilateral control.
- Half of surveyed teens (12–18) admitted to bypassing parental or school controls, mainly through password guessing, changing device clocks, borrowing parents' phones, or using Virtual Private Networks (VPN). Motivations include staying connected with friends, regaining autonomy, accessing blocked educational content, and frustration with over-restrictive systems.
- Bypassing school controls (e.g., breaking GoGuardian or Wi-Fi filters) was common, often justified by students as necessary for productivity rather than rebellion.
- Teens who help parents with tech were also most capable of bypassing: a reflection of high digital literacy rather than malicious intent.
- Teens bypass parental controls not to be defiant, but because controls feel misaligned with real-world use.

The youth interviews reveal a generation navigating an increasingly complex sociotechnical landscape. Adolescents display high functional literacy across digital systems but have limited institutional support for risk management. Our findings illustrate a persistent gap between *institutional models of safety* (e.g., moderation, parental control, digital assemblies) and *youth situated strategies* for managing visibility, privacy, and trust.

While schools, platforms, and parents continue to invest in safety infrastructures — from content moderation to Life360 location tracking — adolescents often report these interventions as *symbolic rather than substantive.*

HOW YOUTH TRUST OTHERS ONLINE

For most participants, safety online began with *who* they were interacting with, not *what* platform they used. Adolescents described a kind of social logic for deciding whom to trust — one based on people and relationships rather than platform affordances. They evaluated credibility through *mutual friends, shared communities,* and *visible overlap* in their social networks. A 17-year-old explained this simple rule of thumb:

"If my friends follow them, I'll follow back. If they don't, I just block."

This practice of relational verification replaced platform-level features such as verification badges or content moderation cues with peer-based reasoning. Adolescents spoke about this process as quick and intuitive, a judgment call made in seconds. They looked for familiar usernames, recognizable faces, or evidence that a new person belonged in their extended friend network.

"Personally, if I get follow requests on Instagram I check to see if any of my friends follow them, because that's an option, and if they don't, I click on their profile and see if it's public or not, and if their name doesn't sound familiar, their name is random, and their profile picture doesn't look normal, then I don't follow them back."

One participant said that a single appearance on a mutual friend's story could determine whether someone was "real":

"If they're in my friend's Snap, I figure they're real."

Several participants emphasized how small cues could be, described as *"reading the room online."* Trust was a fluid, everyday exercise built on shared visibility rather than formal verification.

STORIES OF DECEPTION

Reliance on social cues to decide who to trust online also creates vulnerabilities. Participants described how easily those signals could be manipulated through fake accounts or compromised profiles. A 15-year-old recounted a scam that felt almost personal in its precision:

"They said, 'Can you send me fifty? I'll pay you back tonight.' It sounded exactly like my friend."

This participant sent $50 through Apple Cash, believing she was helping a friend in trouble. When she learned the account had been hacked, the experience shook her initial confidence. She saw it as an opportunity to refine her instincts. Others told similar stories of minor deception including fake charity links, fraudulent giveaways, or clone accounts. Each time, the pattern repeated: confusion, reflection, and adjustment. As one 16-year-old shared:

"Everyone gets tricked once. After that, you start noticing the red flags."

This cycle of exposure and learning transformed small harms into informal lessons. Youth described their digital competence as *earned* rather than taught. Across accounts, youth framed these experiences as necessary rehearsals for adulthood online. They did not expect adults, schools, or platforms to eliminate risk. Instead, they sought to strengthen their own ability to navigate it. For many, this pragmatic view distinguished their generation from their parents, who were described as *"too scared"* or *"too trusting."* Adolescents saw themselves as self-reliant experts in reading digital context, precisely because they had learned through practice.

Relational trust also shaped how teens managed *visibility* across apps. Participants described a layered architecture of disclosure: Snapchat for intimate peers, Instagram for wider social circles, and TikTok or YouTube for public performance. Each layer carried its own etiquette. They calibrated these boundaries

continually, sometimes shifting content between audiences when friendships changed. Safety, in this sense, was not a fixed privacy setting but an ongoing social negotiation.

Participants agreed that keeping profiles limited to known contacts communicated maturity and awareness.

"Having your account private shows you know what you're doing."

Even within private networks, youth-maintained watchfulness. Several noted that they regularly reviewed friend lists, removed inactive followers, and changed usernames to prevent unwanted visibility. One teen said:

"You clean the accounts up, like your room."

Others described maintaining multiple accounts — a public *"main"* and a smaller *"spam"* or *"finsta"* (meaning fake insta or Instagram account) — to partition identity. These practices, taken together, reveal how relational trust structures everyday digital boundaries. Adolescents continually curate who can see them, what they reveal, and how they appear, using social ties as both filter and shield.

TRUST AND GAMING

Some youth interact with strangers on gaming platforms like Roblox. The methods for trusting someone online that worked on platforms like Instagram and Snapchat did not work here. To enable safer interactions, the Roblox gaming community often uses Discord, a messaging platform where, by convention, Roblox gamers trade and negotiate game items because trading directly in-game is perceived as unreliable:

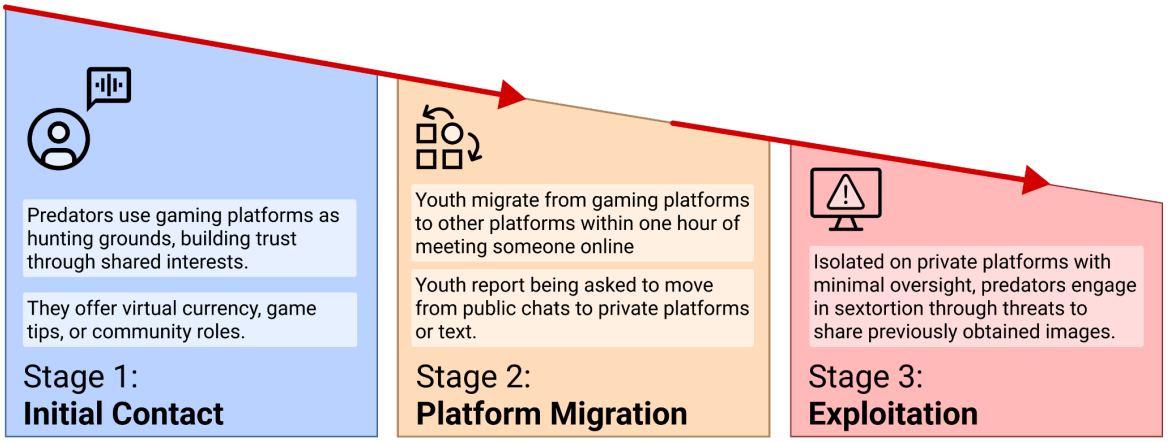
"So, on Discord, you could find people that you can trust. They have these things called vouches. The more vouches you have, the more trusted you are in the community. When you're just going straight onto Roblox, you're trading with people that you don't know at all. And, you can't really trust them most of the time."

For one participant, mistrust in other Roblox players came as a result of exposure to suspicious behavior on the platform. Some Roblox players seem to focus on avatars with *"brighter, colorful avatars"*— signaling association with younger players — and ask questions to try to find out a player's gender, age, or location. Conversely, the avatar design may also signal perpetrators impersonating youth, helping them identify youth players in games. In this study, many participants shared stories in which a stranger would talk with children, ask for personal information and the youth did not report it to anyone. Interestingly, many parents in this study did not understand Discord, were not aware of its safety features, and had perceptions of the platform that did not match real-world use:

"Discord is mainly a business platform for people who work in sales".

THE GAMING EXPLOITATION PIPELINE

Gaming platforms can enable systematic child exploitation through a three-stage process:



Online gaming platforms offer unmoderated voice and text communication that frequently leads to verbal harassment, bullying, and hate speech. Many platforms lack sufficient moderation and reporting tools, allowing persistent exposure to toxic behavior that harms children's mental health and self-esteem. Even platforms with moderation features face challenges, as teens can bypass, or work around, protections through alternative channels like Discord or PlayStation and Xbox Party Chat.

Unfortunately, verbal abuse is often just the beginning. Predatory grooming frequently begins in-game, where perpetrators exploit trust built through chat systems before migrating to perceived private platforms such as Discord or Telegram.

EDUCATION ON DIGITAL SAFETY IS NOT ENOUGH

Youth found that the content communicated to them in curricula in schools encouraged them to avoid social media interactions entirely instead of describing how they might approach a digital presence with more safety.

"It did feel like they weren't as aware of what was happening in social media, and they did talk more, generally about stuff like cyberbullying but not AI and deepfakes. They weren't really talking about how to protect yourself online, just, staying away from social media. I would have talked about keeping your accounts private and not accepting messages from people you aren't friends with."

LOCATION SHARING

Many youths described sharing their location, primarily with family members and a small group of close friends. Parents often viewed location sharing as a safety tool, particularly during daily routines such as commuting to and from school. In many households, tracking applications were used transparently, with teens aware of and agreeing to the arrangement. Some families described reciprocal sharing, with parents also making their own location visible.

At the same time, youth also used real-time mapping features in Snapchat. This feature allows users to broadcast their live location to their network through an interactive map. Several participants reported accepting connection requests from individuals they did not know while keeping this location feature enabled. As a result, their real-time whereabouts could become visible to a broader and less clearly defined audience than intended.

This reflects a clear contradiction. While youth often framed their location sharing as limited to trusted ties, platform design and expanding online networks made those boundaries less defined in practice. Many parents were not aware that location visibility could extend beyond a small circle of close friends, highlighting a gap between family assumptions and the actual functioning of social media location tools.

"I think that it's just a thing people do. Almost everyone that I know that uses Snapchat is like sharing their location. So I can just see all of that. And maybe it's just, like, you can see them on the Snap Map, like, and you know what everyone is up to and who's around."

BYPASSING PARENTAL CONTROLS

As digital technologies reshape everyday life, families are negotiating new forms of visibility, power, and trust. Parental control applications have become a common way for parents to attempt to regulate their children's digital lives. From app monitoring and location tracking to screen-time limits and message surveillance, these tools promise safety in an increasingly complex online environment. The rapid growth of such software reflects mounting concerns about youth exposure to explicit content, cyberbullying, and digital addiction. Even as these apps become more advanced, our research and user discussions show that weak enforcement systems, ethical privacy concerns, and sophisticated youth countermeasures have rendered many forms of digital supervision ineffective.

Parent Motivations and Attitudes. Parents often approach digital monitoring as an extension of care, not discipline. Our research indicates that many of them turn to parental control apps such as SaferKid, OurPact, BrightCanary, Microsoft Family Safety, and Kidslox to oversee messages, app activity, and online behavior. However, parents also express frustration with the limitations of these tools. Many monitoring apps are costly, difficult to configure, or do not work effectively for tech savvy teens. Stricter systems like Aura and Bark, which promise near-total visibility, are often criticized for being invasive or unreliable. This gap between parental expectations and technical reality reflects a deeper issue: the tools meant to bridge generational digital divides often highlight them instead.

Youth Workarounds and Technical Evasion. Youth have developed a parallel digital culture of resistance built on experimentation, collaboration, and technical skill. Online communities on Reddit, an online platform with specialized messaging forums, such as ***r/parentalcontrols*** and ***r/teenagers*** contain hundreds of posts sharing detailed methods for disabling or removing parental control systems. Common bypasses include manipulating device settings to block server communication, exploiting the Android Accessibility Menu to reopen locked applications, and uninstalling monitoring software.

On iOS devices, youth have discovered URL manipulation exploits in Screen Time, where appending a permitted website's address to a blocked one allows hidden access to restricted content. Others use messaging apps like iMessage or WhatsApp as covert browsers, sending themselves links that open inside in-app browsers even when Safari is disabled. These methods display a remarkable degree of technical literacy, demonstrating that young people are not passive recipients of surveillance, but active learners navigating — and reconfiguring — the systems designed to control them.

TECHNOLOGICAL CONSIDERATIONS FOR SPECIAL POPULATIONS

Throughout this research, we have included adult participants (e.g., parents, educators, and law enforcement) who support youth with special needs. For students with special needs, digital technologies hold great promise; however, these technologies can also pose a unique set of problems. In recent years, diagnoses of cognitive and developmental disabilities have progressively increased [8, 9], expanding the responsibilities of educators and policymakers to facilitate specialized learning environments for these populations. Technology can enable personalized learning experiences and individualized instruction. While AI-assisted interventions can be effective, they also must be navigated with great care.

Parents and educators described both the enhanced learning opportunities as well as the risks presented via emerging technologies and the need to readily identify misinformation. Youth with disabilities often relied on technology use for assistance with homework more than their peers, leaving them more vulnerable to the challenges that come with that usage. Moreover, parents of children with special needs reported fewer risk management practices than other parents in this study.

Parents

Key Findings

- Perspectives of social media platforms often did not align with the actual risks posed by the platform features.
- Parents struggled with identifying platform features and vulnerabilities.
- Many parents became aware of digital harms through online sources or online communities.
- Parents often perceived gaming platforms as safe, unaware of their risk as well as their parental control features.
- Parents did not feel as informed about AI risks, and were not comfortable with their children seeking advice with chatbots.
- Parents expressed frustration with a lack of institutional guardrails surrounding AI and technology education for their children.
- Parents often underestimated the likelihood of sextortion and were unfamiliar with the risks for youth.
- Many parents felt that schools did not support paper-based assignments even when youth were contending with digital safety issues.
- Parents of youth that experience sexual violence stemming from online interactions described how things quickly spin out of control and can lead to self-harm, and addiction.
- Some parents helped their youth buy and sell gaming items online outside of the gaming platform, unaware of the risks to their own safety.

Parental Protective Practices:

- Some **methods used to monitor children's phones**:
    - Bark App
    - Apple's Screen Time Feature
    - Sharing accounts (like TikTok) with children
    - Having passwords
    - Physically asking for phone at will
- **System flaws:** Many parental-control apps still have vulnerabilities (e.g., local VPN privilege abuse) – "*don't set it and forget it*"

Youth Workarounds:

- Common methods:
    a. Password guessing / observing parents' codes
    b. Changing device clocks
    c. Using parents' phones
    d. Installing VPNs
    e. Screen recording parents inputting passwords on youth's phone
- **Motivations:** staying socially connected, autonomy, academic needs
- Teens with **higher digital literacy** (those who help parents with tech) were **most capable** of

bypassing limitations

TECHNOLOGY USE THROUGH LIVED TRAUMA

Parents in this study described managing digital risk as a form of crisis response rather than routine caregiving. One parent situated her vigilance toward AI and online platforms within her experience as a survivor of *"childhood sexual abuse, human trafficking, domestic violence, (and) gang violence*". She explained that understanding technological risk had become *"a moral responsibility"* tied to protecting both her clients and her own children. Another parent — managing a household with multiple neurodivergent children — described online safety as *"daily triage."* Both narratives frame safety as emotional and moral labor performed in the absence of structural protection.

PERSPECTIVES OF SOCIAL MEDIA

Parents gather sources of information surrounding popular social media apps from various online sources, including social media apps themselves. One participant described that they learned of the risks of Roblox while browsing social media and garnering the perspectives of other users:

"When I was using social media people were saying that something was going on with Roblox, and they were able to simulate or do inappropriate things or something."

These perspectives in turn influence whether parents would allow their children to download or interact on these platforms, particularly when the information could manifest as potential threats. Parents also expressed wariness towards malicious users on social media platforms that could manipulate their appearance and profiles in order to gain access to more vulnerable groups.

"The biggest issue with technology and social media is that many people online are posing. They're creating false perceptions of reality."

Additionally, parents' conceptions of platforms and online spaces misalign with actual experiences on the platforms or internet, often finding the reality to be more daunting and dangerous.

"I never knew how bad the Internet was, how powerful it was, and how much it affects teens until I dealt with it myself."

GAMING

Misconceptions and Platform Deception. Parents had a broad array of perspectives regarding what was safe and what was harmful. Many parents described having strict rules and limitations around social media apps such as Instagram and Snapchat, but limited rules around games. For instance, many parents allowed young children aged 4 and older to play videogames.

Some parents expressed skepticism toward *"child-safe"* platforms such as YouTube Kids, Roblox, and Minecraft. They identified how these systems rely on self-reporting and keyword tagging rather than verified moderation. One mother shared:

"Creators can word the description so it looks child-safe," yet videos still contained *"cocaine, sex, (and) partying. You can essentially upload content for YouTube Kids that would meet the criteria, as long as*

you're accurately wording the description, the title, and things like that. So, if a content creator wants to attract the attention of children for whatever the reason, they can."

Communication Channels and harms. In-game chat, Discord, and streaming environments emerged as chronic sources of harm. One parent recalled that their daughter exchanged Snapchat information with a stranger that she met on Discord and was asked to send nude pictures and videos. An educator described a child lured to a physical location after disclosing her school name online. Both reported that parental controls *"don't work with the game chats"* and that *"there's no vetting of age"*. Due to these minimal controls, it is easier for perpetrators to communicate with children without parental awareness.

Law enforcement investigations were met with challenges due to cross-jurisdictional limits (*"it was from Australia, some guy in Australia"*) as youth engaged online with people from a wide range of geographical locations. These experiences shaped parents' perception of law enforcement as structurally powerless, constrained by obstacles in the digital world that do not exist in traditional investigative frameworks.

PARENTS' PROTECTIVE PRACTICES

To fill this vacuum, parents took the digital safety of their children into their own hands by implementing systems like the following:

"One mother described linking all devices to her Google account so deleted photos "still go to my Google Photos". These tools offered visibility but no guarantee of safety. Parents recognized that "we can put all the parental controls we want, but it's the people adding the content."

Parents note that they have found it difficult to enforce the protections of parental monitoring controls, as youth are often able to work around the protective measures, no matter the methods used to impose them.

"It just feels like there has to be a better way… we have all this technology, and yet… every time we try to use any kind of parental controls, they work for some things, but there's a million loopholes that you can't possibly keep up with."

AI AND SYNTHETIC MEDIA AS EMERGING THREATS

Parents described emergent threats from generative AI and deepfakes. One warned that a chatbot *"has told someone it was okay to kill themselves,"* linking this to broader concerns about algorithmic manipulation of vulnerable youth. Another parent recalled getting upset when their daughter turned to ChatGPT as a substitute for her therapist.

"This (ChatGPT) is not a licensed mental health professional that went to school and studied. It is an electronic device."

Two parents worried about voice synthesis enabling impersonation — *"If it can sound like me, it can tell my kid anything."* These reflections extend abuse-of-trust threat models into synthetic identity attacks and highlight how emerging forms of deception may evade both platform moderation systems and existing law enforcement classification frameworks.

SEXTORTION AND COERCION

Several participants reported experiences with sextortion incidents involving their children. One parent described discovering explicit photos through linked cloud backups in which there were threats to send out the images if more were not sent. Another parent recounted her daughter receiving unsolicited sexual images online accompanied by demands that she send explicit images in return. In these cases, reporting mechanisms failed to provide meaningful relief:

"We had to leave the content on the tablet for 90 days while (police) tried to establish where it was coming from".

When law enforcement traced the perpetrator abroad, *"they couldn't track it or nothing."* Parents thus experienced policing as procedural but unsuccessful — a bureaucratic process that documented harm without preventing or resolving it. The result was chronic exposure to unresolved trauma through forensic preservation of evidence.

Parents also highlighted how social climates make more youth more susceptible to engaging in soliciting or sending nude images, which could in turn lead to sextortion.

"Some kids are more impressionable than others. Some may want to just do what their friends are doing, so they're not feeling left out or getting made fun of. They can fall into sextortion."

Educators

Key Findings

Youth Monitoring:

- Participants shared that **monitoring** takes place throughout the school day **in the digital and physical world.**
- **Digital:** Schools receive alerts if youth misuse school-owned equipment or services (e.g., email, browser searching, etc.).
- **Physical:** Educators at times overhear youth speaking about harms or are approached directly by peers concerned about other students.

Barriers Educators Face:

- There are many **legal barriers** that limit how and how quickly schools can respond to reports of digital harms against youth.
- Educators experience **training barriers** stemming from a lack of time and resources to dedicate towards in-depth understanding of digital safety material.
- They also shared that it is extremely **difficult to stay up to date** with new youth harms or areas of concern.
- Participants stated their concerns with **youth workarounds** to school-implemented restrictions and blocks.

Tensions Between Educators and Parents:

- Educators described feeling **the weight of protecting youth's safety** and called for parents to become more engaged to help alleviate pressure.
- Some educators identified a **dire need for youth digital and physical safety resources for parents** to mitigate the questions they receive.

Educator Training Needs:

- There is a need for trainings focused on **how to identify concerning behavior** or change of behavior in youth and appropriate next steps.
- Educators stated that they need resources on **how to engage youth's families** when harms arise.

- Educators requested trainings on how to have conversations about digital safety and wellness with students as well as resources for **how to help kids understand the importance of these topics and rules** (e.g., Bell-to-Bell, etc.).

Educators in this study included teachers, principals, guidance counselors, consultant and teacher assistants, and outreach and education specialists. 10 participants were also parents and shared relevant experiences they have had with their children. They worked in various types of schools and programs, including public, private (religious and non-religious), charter, Vocational/BOCES, CTE, virtual high school programs, a homeless youth program, family planning service provider and victim service provider. Educators primarily worked with middle and high school aged students, including special education and alternative education programs.

The 24 educators interviewed in this study shared their thoughts on major influences on youth behavior, types of harms youth face today, schools' current responses and barriers to youth harms, and knowledge gaps they believe need to be addressed in order to effectively protect youth. Participants provided insight on the youth groups they felt are at high risk for harm and detailed the type of training they need in order to support their students. They also identified the ways their students are using technology and platforms that are worth noting.

INFLUENCES ON YOUTH'S BEHAVIORS

Participants disclosed their views on how mainstream and social media, COVID, and the heightened loneliness youth feel has influenced their students' judgements around communication and connection seeking.

Mainstream and Social Media. According to educators, social media has a large impact on students' self-expression and communication skills. With regard to communication, educators felt that the media youth consume influences their perspectives on what experiences or behaviors are normal and impacts whether they come forward when in concerning situations. Participants also found that instead of internally processing their feelings, youth often shared them on social media without anticipating potential consequences.

Loneliness. Educators identified patterns in students feeling incredibly lonely and/or ostracized at school leading them to seek connections outside of their peers and/or online. This in turn increases the risk that they will face harm. Although students may recognize the risks of seeking connections with people they are not familiar with, educators shared that many times the promise of finding someone who cares for them outweighs concern for the potential harm they may face.

"I think that they [students] know the dangers, but they accept that because they're so lonely … they don't have any thoughts of having any relationships with people inside the school because they've been ostracized for years, and they're looking for anybody that will give them attention."

These behaviors are often targeted by predators who feed into a youth's need for connection. Educators shared that though they may warn students to be careful, they still see cases of this happening and deal with the fallout.

YOUTH DIGITAL SAFETY EDUCATION

Educators described different sources they use to stay up to date with the platforms and technology their students are using. Participants also showed varying levels of knowledge regarding how to discuss youth digital safety effectively with their students. In terms of the former, some participants shared that they

educate themselves through sources such as YouTube, news/social media, and occasionally their students. Information about harms youth face is also often supplemented by school resource officers, principals, and local law enforcement.

"Some awareness around [deepfakes], more through the media and conversations that we have with our school resource officers as well and with local law enforcement. The school has not gone out and done massive amounts of work on it."

The extent of training or guidance educators receive regarding how to teach youth digital safety to their students varies based on the type of school or program they are in. Educators working directly in schools described limited formal training on youth digital safety education though in some cases they were encouraged to talk about digital citizenship.

On the other hand, an educator described receiving extensive training on how to teach kids of different age groups (middle and high school) about topics such as media literacy and the dangers of sexting.

"We do a 2-day training with youth which focuses on how to teach a program, there is another program which is our longest and takes 2 weeks. I've also completed training on how to teach. We are also provided with additional research tools that are recommended and include books and webinars."

MONITORING OF YOUTH

Educators shared the different ways they monitor youth's safety and stay aware of what is happening with students, with sources including youth themselves, peers, adults/guardians, and law enforcement. Some schools have technical systems in place, such as alerts that notify the Information Technology specialists and the principal if there is a misuse of the school email or browser, a self-reporting system so students can share any threats they identify to themselves or others, and a referral system for teachers and staff to keep track of students that may need to be followed up with (e.g., sleeping through class, working when not supposed to, has bruises). Occasionally, educators are made aware of a harm a student is experiencing because they overhear it happening or peers of the youth come forward to express their concern on their behalf.

"... usually it's their friends that tell on them, and… it gets to us… a friend, or someone observed it, something is different, they're dressing differently, they're behaving differently…"

HARMS TOWARD YOUTH IDENTIFIED BY EDUCATORS

Educators shared various anecdotes about the types of harms they are aware their students have experienced. These harms include escalations of online conflicts to physical fights, as well as inappropriate experiences with adults being victims of non-consensual intimate images (e.g., boyfriend recording sexual activities to post on OnlyFans without student's knowledge), extortion/sextortion, and intimate partner violence. They shared being aware of mostly peer-to-peer harms, acknowledging that other harms are occurring but that they just do not know as much about them.

Relevant Platforms. Participants noted that Instagram, Discord, and Snapchat are popular amongst students. One educator recounted a time when a student shared that they removed themselves from a Discord group with some younger friends of theirs because they feared getting in trouble if associated with the illegal content the younger students were sharing. The educator described the dynamic directly:

It's groups of people on Discord, one or two of them are 18 or older, still in high school, but they feel they can no longer be part of the conversation because the younger students are participating in behavior that involves sharing troubling content. They would never tell me what it was, but they always said, 'It's illegal. I could be in a lot of trouble if I got caught online with these kids, so I'm not going to talk to them anymore.'"

BARRIERS TO SCHOOLS' RESPONSE TO HARM

Legal Barriers. Some educators expressed there were a lot of legal barriers with how schools can respond to and discuss digital harms against youth. These educators believe that law enforcement has the most authority in monitoring online activity, but they themselves have limited access in monitoring their student's digital lives.

"If a student is being manipulated or being exploited on one of these sites, one would have to go through a local law enforcement screening office. Even … the school resource officers that we have, have to go through a centralized office before they have access to that … We would not be able to go there, it would be a violation of board policy, etc."

Training Barriers. A couple educators signaled that they simply do not have the time or resources to stay up to date with all the concerns youth are facing. Almost all of the educators indicated there was at least some training on digital safety made accessible by their school system, but they do not have enough time to be trained as in-depth in these topics as they would like. Some have trouble navigating how to respond to student digital safety concerns that happen outside of school.

"There is so much to navigate with what is happening in the world outside of school, and with technology… we can't keep abreast of any of it… We are ill-equipped in terms of time and understanding to navigate it. But we're dealing with it because it's been brought to our doorstep. We are grossly inadequate when it comes to protecting our children."

Youth Workarounds. Schools that participants are employed at often have strict restrictions on content and sites their students can access, especially on school-owned technology. Some educators have expressed concerns that regardless of what school restrictions are in place, youth will continue to find means to bypass them, similar to parental controls.

KNOWLEDGE GAPS IDENTIFIED BY EDUCATORS

With Parents. Some educators expressed feelings that parents are naive about the "*horrors that are out there*" and need to take a more active role in monitoring the online interactions of their children in order to protect them. They shared feeling overwhelmed by the responsibility placed on schools and educators to keep students safe, when in reality they themselves are struggling to learn and stay updated on the harms affecting their students.

"We need to do a … far better job protecting these students and we're far from there … (we need) more media attention about this topic, more generated references and articles about this so that parents can be made aware that if they're looking at schools to be the bastions of support and gatekeepers of this it's not happening there [at school]... They need to reclaim their role in the raising of their children."

With Students. One educator shared that they think students recognize when something is wrong, but do not know if students know when to seek help or that it is ok to say something. They expressed wanting more guidance on how to inform kids of the importance of following certain rules (e.g., no cell phones in school, etc.) as it might help kids follow them.

"...helping the kids understand the why … there's no real clear process… we tell kids all the time, you do certain things, you get into a fight, you bring drugs into school, you destroy property, you're not only got a school issue, now you've got a legal issue as well … those are very clear-cut things that we can tell them, but when there's something happening online, where are those lines, and who do we go to to help them? We really need to help them navigate it and understand it"

With Mainstream/Social Media. Engagement with mainstream social media platforms was also discussed as a potential channel for awareness. One educator suggested that mental health messaging should

appear on social media at a frequency comparable to commercial advertising in order to reach parents and students and reinforce the work done by educators:

"… if we [educators] were part of an algorithm that flooded their [parents, guardians, and students] social media the way Temu and all of these other things do … that would help in terms of building better connections, providing support for educators and for families."

Law Enforcement

Key Findings

- Attachment disruptions can heighten vulnerability; participants commented that youth without stable, secure caregiving relationships — particularly girls — may be more susceptible to unsafe forms of adult attention in digital spaces.
- Officers and educators should distinguish between intentional misconduct and behavior shaped by underlying neurological or developmental conditions. Misinterpretation can lead to punitive responses where support or accommodation is warranted.
- Stigmatization and limited support infrastructures inhibit reporting and weaken prevention efforts. When disclosure pathways are perceived as punitive, adolescents are less likely to seek help.
- Trauma is often cyclical and normalized within peer contexts. Several adolescents described only later recognizing prior experiences as abusive, sometimes years after patterns of harm had begun. Delayed recognition complicates intervention and reinforces silence.
- Normative models of healthy relationships are inconsistently communicated by institutions and caregivers. In the absence of explicit guidance, youth may rely on peer norms, increasing susceptibility to coercive dynamics and unhealthy interactions.
- Participants reported that nonconsensual sharing of intimate images is frequently minimized and normalized. Youth often underestimate the legal, relational, and psychological consequences, particularly when exposure to such behavior is routine within school environments.
- Law enforcement professionals noted that reported cases of cyberstalking among youth are comparatively low, which they attribute in part to the normalization of persistent monitoring and intrusive digital behaviors.
- Law enforcement are seeing more cases of peer-to-peer sextortion.
- Known cases of peer-to-peer sextortion have been elaborate, larger scale attempts (entire class) and can include distribution on external platforms such as Telegram.
- Young males are disproportionately victimized in peer-to-peer sextortion, often through social media, gaming, and peer networks.
- Platforms including Discord, Snapchat, Reddit, and online gaming environments have been identified as spaces that pose heightened risks for adolescents due to the ease of unmoderated interaction, content sharing, and anonymity.
- Perpetrators often migrate youth from public or semi-public digital spaces (e.g., social media platforms, gaming chats) into perceived private communication channels to increase control and reduce detection.
- Perpetrators frequently use text-based manipulation to obtain sexual images from victims without revealing their own visual identity.
- Financial transactions are commonly facilitated through peer-to-peer payment services with initial payments typically ranging from $20–$50.

Law enforcement professionals included school and campus-based safety officers, safety directors, local law enforcement, consultants, community supervisors, and investigators for crimes against children. 14 were interviewed for this study and described an environment where vulnerable youth face growing exposure to digital and interpersonal harm. Law enforcement professionals worked in suburban, rural and urban centers.

Our research reveals how behavioral issues, family instability, and the widespread availability of technology intersect to create cycles of risk that are difficult for law enforcement professionals to contend with or interrupt. They described students with behavioral disorders, developmental disabilities, and histories of trauma, many of whom find validation, attention, or connection in unsafe online spaces. Their experiences highlight persistent gaps in digital safety training, limited institutional capacity for intervention, and the emergence of new threats linked to AI and evolving online platforms.

Participants framed their role as a mix of enforcement, counseling, and mediation among students, parents, and other professionals. Respondents, including school resource officers, described a hybrid practice of enforcement and care work. Collaboration with parents was inconsistent, some cooperative, others adversarial. Interventions extended beyond disciplinary action to include mentoring, emotional de-escalation, and goal setting.

Sustainable youth digital safety programs should formalize these hybrid roles — integrating law enforcement, mental-health, and educational staff into coordinated response teams. Training should prepare officers for counseling-oriented interactions while providing clear escalation pathways for severe online exploitation cases.

DISTINCT SOCIAL GROUPS CORRELATE WITH DIFFERENT LEVELS OF THREATS

One law enforcement professional noted that each individual youth can retain multiple, independent groups of friends for different social purposes, ranging from academics to extracurriculars to entertainment. Within these spheres, different levels of threats can manifest depending on the environments they are interacting in and the level of trust they have with the people they encounter and frequently communicate with.

“We see multiple groups of friends within a single person, meaning there's the group of friends that they have in school, there's the group of friends that they hang out with, there's the group of friends that they live near, there's the group of friends that they're involved in whatever extracurricular activity they're involved with, there are kids that they game with, there are kids that they engage on other social media platforms with.”

Anonymous individuals pose stronger threats, sometimes initiating dangerous relationships with youth, leading to potential self-harm and other levels of violence.

“They have other groups of friends that they're engaging with that are completely unknown or anonymous, and we've seen that in actual student cases that we've dealt with. We have had groups like 764 that are out there trying to get vulnerable populations to self-harm, get them to that level.”

In many cases, predators **employ social engineering tactics to appear as a more legitimate, validated person that the youth may know.** Available information like a common school name or mutual friends allows predators to slip past precautions that youth would normally take around unknown individuals.

"After a perpetrator finds a victim, what they'll do is they'll do some social engineering to figure it out and to create a mirrored profile of a youth appearing to be in this same school district. Then they do the friend request, and request some other friends that are in that school, maybe steal and repurpose some pictures, which have been easier to obtain or create with AI. They create this fake profile and this fake persona and the coercion starts."

Additionally, participants described a structural feature of online gaming environments: social interaction is often detached from offline identity. In gaming-based peer groups, youth may interact extensively, cooperating, competing, or communicating regularly without realizing that the other person is a classmate or someone they encounter daily in physical spaces. This disconnect between online and offline identities produces parallel social worlds that rarely converge unless deliberately disclosed. As one youth participant explained:

"We might have been playing on Fortnite together, but they could be sitting next to each other in the classroom, and you would not know it. You could be sitting across from me in a lunchroom, and I would have never acknowledged you, but meanwhile, you and I are, you know, in the Sims game together."

Youth may also be more trusting of individuals whom they meet exclusively online due to the prevalence and accessibility of technology and social media in this age — youth are accustomed to spending large amounts of time online in spaces where they may be more comfortable interacting with someone virtually than physically.

"I think that a large part of that is that they have grown up disconnected from face-to-face contact. And they trust that the person on the other end of that text communication is who they say they are."

THE BROADER PATTERN: CYCLES OF VICTIMIZATION

Another law enforcement professional, expanded on this theme of cyclical victimization. They argued that many "*offenders*" or "*problem youth*" are, in fact, reproducing the only models of behavior they have ever known.

"Sometimes they're victims themselves. This is something that they grew up with. This is all they know, they think it's normal."

The participant's description paints a grim developmental trajectory: children exposed to abuse from early childhood internalize those dynamics and often reenact them in adolescence — sometimes unconsciously.

"It's taught to them by some type of peer, whether it be a parent, or a teacher, or a guardian, or… could be anyone. It could be the neighbors next door, you just don't know."

What makes this cycle particularly destructive is how long it takes for these youth to recognize that their experiences were abusive at all. Years — sometimes a decade or more — can pass before realization dawns:

"It takes them a long time to realize that, wait a minute, I've been a victim. They're 15, 16, and 17 years old, and they're finally learning that this has been a problem, and they've been doing this to me since I was 5 years old. So now we have 10 or 15 years of abuse under the belt before they realize something's wrong."

Their testaments underscore both alarm and fatigue — a sense that risk is not a possibility, but constant, structural, and self-reinforcing. The system is reactive, not preventative, leaving law enforcement to deal with youth that carry trauma from prior experiences as victims.

TECH-FACILITATED HARMS AND PEER-TO-PEER SEXTORTION

Tech-facilitated harms are not limited to acts of sextortion, but often can stem from social discourse and word of mouth at school. In many cases, it is evident just how fast words or images can travel around in a social setting among youth.

"She said there was a picture of somebody, some girl, and then a list going around the grade about who's hot, who's hotter, who's this, like, kind of in that frame, sexual-wise, like this young girl is, like, basically, they're passing around a list, and people are signing off on it or people are saving the picture to the phone"

Perpetrators may take an array of approaches to solicit images from youth. One participant describes a scenario in which the perpetrator uses pornography to drive the youth to send them a desired image or video.

"I think it's, case by case, for the simple reason that… These kids have been shown pornography, to kind of show that 'this is what I want you to do', then the suspect makes the child reenact what they see in the video."

These harms have a wide range of risks spanning from social humiliation to sextortion. Youth are concerned with the risks pertaining to their social capital, and how their actions online may negatively affect their friendships or relationships at school. Perpetrators often exploit this vulnerability when looking for targets of sextortion.

"Recently, they were getting reports middle school grade boys were getting added on Snapchat from an account that was posing as a female. The user of the account asked for the youth to send photographs engaged in private sexual acts. Then, after they got the photograph, they started to extort them, saying, I'll send this out to all the other boys and girls in the school unless you send me a hundred dollars over Apple Pay or a $100 gift card from Target. This turned out to be peer to peer."

As previously described, there are also multiple instances reported of attacks on youth originating from their peers. Hence, not only are youth susceptible to harm from strangers online, but also from those who are closest to them.

"So I had two cases, most recently high school age kids, girls who were the perpetrators. They took someone in their friend group, put her face on a naked body, started to report that it's her, and then sent it out."

"We had a middle school case of a 7th grader male sextorting his 7th and 8th grade peers, getting photos, videos of them, and then threatening to send it to the school if they didn't send money. The classmates did send money, often close to $100."

"In recent cases of peer-to-peer sextortion, we have seen boys impersonating girls. They create a fictional account and ask for pictures and then sextort peers. In one case it was for money and in another it was for more photos."

In the cases of peer-to-peer sextortion, law enforcement stress the lack of accountability and ramifications that follow, even citing an experience where a youth researched the potential for liability for sextortion prior to committing the crime.

"Kids assume there will not be consequences. For a youth doing this, there pretty much is none. One kid knew because of his age that he wouldn't get in trouble. He actually did his own research."

ADULT MISCONCEPTIONS AND DISCOMFORT WITH DIGITAL HARMS

Law enforcement professionals have found that school districts and parents or guardians focus efforts on physical safety precautions in comparison to the growing number of threats residing in digital spaces.

"They have a huge emphasis in our area on not drunk driving. I mean, they put in a lot of effort, but there's none being invested into cyber-stalking, cyberbullying, the use of technology to really just ruin these children's lives, because I'm seeing it happening."

In some cases, it is not that the parents or school figures are unaware of technology-facilitated harms, but rather the discomfort with having conversations with their children about potentially taboo or explicit topics.

"Learning… to talk about the hard things… to have the conversations of, if you make a choice to take a picture of yourself that other people shouldn't see, and you put it out there, it's never coming back. And it

will be out there forever, and it will follow you, and having the uncomfortable conversations… some parents don't want to have those conversations with their kids, and showing the consequences of actions that they don't even fully grasp themselves because they're not developed in their, you know, thinking."

When youth are left without general guidelines on healthy relationships, both in the physical and digital worlds, they are more susceptible to being exploited in either. Without proper trainings or conversations with adult stakeholders, the only baseline youth have for normal behavior is through the interactions they have experienced. Hence, conversations surrounding acceptable and unacceptable behaviors need to be clearly communicated for safer, healthier interactions in both the physical and digital worlds.

Key Stories

In this work, we heard several stories from stakeholders that highlight the need to look at this issue as a form of gender-based violence.

ONLINE SEXUAL EXPLOITATION AND ABUSE OF YOUTH USING TECHNOLOGY

Law enforcement officers described the volume of child sexual abuse material (CSAM), trafficking, and sextortion cases as overwhelming and increasing. One officer explained the frequency and severity of exposure to such cases:

"Daily. Multiple cases a day. It's out of control. We don't have nearly enough manpower to combat this. It's a pandemic. It's very bad. Social media and the internet has exploded this. It's not getting better. We can investigate and make the arrest. We do what we can do. But there's always somebody else out there doing the exact same thing. We just haven't caught them yet. It's out of control." – Law Enforcement

Officers also report cases involving youth who leave home to meet individuals they encountered online. In one session, a law enforcement officer discussed incidents of children running away with people they met through internet platforms.

Online group environments can also become spaces where exploitation spreads rapidly, often involving both youth and adults posing as minors. In one investigation described by law enforcement:

"A Discord group of students was discovered sharing nude images. A student reported the group to a teacher. During the investigation, authorities found that adults were posing as children within the group and were receiving the images. Approximately 20–40 minors were involved." – Law Enforcement

ONLINE SEXUAL EXPLOITATION AND ABUSE OF GIRLS USING TECHNOLOGY

Participants also described gendered patterns in these incidents. In cases involving girls, respondents reported multiple instances in which girls were approached online and solicited for explicit images. One educator described her daughter being contacted by an adult posing as a peer:

"My younger daughter (16) has been approached by predators. You know, that don't even supposedly live in this state, that… You know, tried to coerce her. Luckily, you know, it was kind of, you know, after the fact that she came to me, but… like, you know, she said, it's… there's… I feel like there's gotta be a better way to keep them safe" – Educator

Another educator described a similar incident in which the perpetrator misrepresented their age:

"The predator asked for sexual images, the daughter thought it was someone her age. Her parents went through the messages and could tell it was an adult grooming and not a child." – Educator

Participants often reflected on the persistence and manipulation of perpetrators coercing youth.

"It took days, not, like, hours. It didn't go from let me be your boyfriend to send me pictures. It was talking, back and forth, for days before anything started to turn, inappropriate and, more than just regular pictures, and wanting more explicit content." – Educator

There were also cases of predators attempting to reach a victim in the physical world, and even kidnap them:

"A 14-year-old girl was sending and receiving sexual images to a 25-year-old, who she thought was 15. The 25-year-old had kidnapped two other girls and was trying to get her to run away and go to him, to kidnap her as well. They were actively planning on her running away and the 25-year-old was caught doing this to her while the investigation was happening" – Law Enforcement

Law enforcement also described cases involving organized sextortion networks. One officer recounted an incident in which a girl was targeted after an offender impersonated one of her friends:

"*There was a girl sextorted by 764 and told to cut herself or her photos would be shared. She was targeted by 764, after someone reached out to her initially impersonating her friend*." – Law Enforcement

ONLINE SEXUAL EXPLOITATION AND ABUSE OF BOYS USING TECHNOLOGY

Contrasting from technology harms against girls, boys were more targeted in cases of peer-to-peer sextortion. One law enforcement professional highlighted a scenario where a youth as young as in middle school may be vulnerable to being sextorted after interacting with an individual, particularly in a gaming environment.

"Sextortion has come up in some of the cases. Unfortunately, it seems to be young male middle schoolers who start interacting with someone, sometimes in a group setting, like gaming, for example, in a chat group. Then someone will start a side chat, strike up a conversation and start sending videos or photographs, and then requesting it from these young males. They would send it. The next thing you know mom and dad are starting to see money out of an account, or so forth, and we end up finding that these young juveniles are sending money because they're being sextorted." – Law Enforcement

Participants also reported emerging concerns about the use of generative AI tools among students. One educator described incidents involving the creation of deepfakes targeting girls:

"We are seeing more cases in which boys at school create deepfakes of girls possibly due to access to the new apps." – *Educator*

ONLINE SEXUAL EXPLOITATION AND ABUSE OF LGBTQ YOUTH USING TECHNOLOGY

There were also reported cases of perpetrators intentionally targeting vulnerable youth in specific communities, such as LGBTQ:

"I had a transitioning individual who was a juvenile in one of the sex trafficking cases that I worked, actually, and there was a lot of sex trafficking happening where we lived, they were preying on vulnerable LGBTQ juveniles who were very susceptible to manipulation." – Law Enforcement

TEEN INTERPERSONAL VIOLENCE

Stakeholders described relationship dynamics in which constant digital access and surveillance were normalized rather than recognized as potential warning signs. Continuous connectivity was often interpreted as commitment or intimacy, even when it reflected dependency, control, or escalating coercion.

"We had a student who remained on FaceTime throughout the day with a girlfriend who lived elsewhere. There was a constant expectation of communication. This level of continuous availability was described as normalized within the relationship." – Educator

"In another case, a female student formed a relationship online with a girl almost eight years older. The older partner demanded constant phone contact and became controlling and violent. After an incident in which she physically assaulted the student, the parents tried to intervene. However, the student would not end the relationship with the older partner, reflecting the intensity of coercive control and fear of relationship loss." – Educator

Youth have even reported experiences where partners would use coercive behavior and relationship status to gain access to the youth's devices, bypassing consent.

"I didn't want to give him access. My boyfriend wants to know I'm not cheating on him, so he made me give him my passwords so that he could see everybody I'm messaging. I would say that that's not true consent when you're being, you know, manipulated into doing it. I don't want my boyfriend to break up with me, so if this is what they're demanding of me, I'm just going to do it. – Youth

Location-sharing technologies were also described as contributing to the normalization of possessive monitoring behaviors among youth, potentially increasing risks related to interpersonal violence. One law enforcement participant explained that constant location sharing can obscure early signs of stalking or coercive control:

"I think that the reason we don't get a lot of cyberstalking cases is that we have a huge disconnect with this younger generation on what stalking even is. Because you have apps like Life360, they share their locations with their whole friend group, and they share everything, and they don't realize that. Sometimes, people don't need to know where you are all the time. They know everywhere you've been, and how fast you traveled there. When we could be identifying cases where maybe a teenager has an intimate partner who is a little too possessive, they don't report it because they think it's normal." – Law Enforcement

Participants also described situations in which constant connectivity enabled controlling or surveillance-like behavior among youth. One law enforcement participant recounted a case in which a teenager remained connected to another individual through FaceTime for most of the day:

"Sometimes we get calls where things have boiled over at home, and maybe our road patrol ends up there. We had a mom who was trying to take her daughter's cell phone away as a punishment. The child got very upset and had a tantrum. The mom learned at that moment that they're on FaceTime probably 20 out of 24 hours a day. And the mom wouldn't even be aware of it, because the phone would be in the daughter's pocket, or whatever, and she wouldn't even know that he's listening to everything that's happening in this child's life." – Law Enforcement

Conclusion

These insights gained from the experiences of real New Yorkers will serve as a foundation for future work on safeguarding youth and the public from these potential harms and vulnerabilities. Technology can feel scary, especially new emerging technologies and how they may impact youth. However, there are ways to

protect youth online so that they can enjoy new technology while staying safe. We conclude this report with some actionable ways caregivers and other stakeholders can promote safe online practices while nurturing consent, digital autonomy, and the growing independence of youth in their care.

For more information on technology-facilitated gender-based violence, please visit opdv.ny.gov/technology-and-gender-based-violence.

What You Can Do

What can you do to monitor social media and community data practices?

- Set explicit norms with family and community members about posting images of your child. Disable tagging and remove geolocation metadata where possible.
- Determine whether school-affiliated accounts are public. If public, assess what student identifiers (names, jerseys, schedules, locations) are exposed.
- Audit your privacy settings. Restrict who can view, download, message, or reshare your content.
- Inventory devices and services with access to family data (phones, tablets, smart speakers, gaming consoles, cloud backups). Identify what data categories are collected and retained.
- Evaluate parental monitoring apps critically. What telemetry do they collect? Where is it stored? Who has access? What are the breach implications?

What can parents do?

- Discuss digital footprint as data persistence and aggregation, not just reputation. Content can be scraped, indexed, and repurposed.
- Model consent before sharing images of your child. Normalize asking and declining.
- Review communication channels within games (text, voice, livestream). Disable unnecessary features and use platform-level parental controls.
- Avoid excessive surveillance that centralizes sensitive data in third-party systems without clear security guarantees.

What can schools and administrators do?

- Adopt a student curriculum on digital literacy.
- Require documented consent before publishing student photos or personally identifiable information on extracurricular accounts.
- Default accounts to private when feasible; disable tagging and limit comments.
- Avoid posting travel schedules, real-time locations, or team rosters that enable inference of a minor's whereabouts.

What can the community do?

- Align parent-to-parent expectations about reposting and tagging.
- Encourage educator-to-educator discussion on data minimization in school communications.
- Establish clear parent–educator channels for reporting impersonation, doxxing, or online coercion.

References

[1] Freed, D., et al. (2023). Understanding Digital-Safety Experiences of Youth in the U.S. *In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 191, 1–15. https://doi.org/10.1145/3544548.3581128

[2] Finkelhor, D., Turner, H., & Colburn, D. (2022). Prevalence of Online Sexual Offenses Against Children in the US. *JAMA Network Open*, 5(10), e2234471-e2234471. https://doi.org/10.1001/jamanetworkopen.2022.34471

[3] FBI. (2025). Sextortion. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion

[4] FBI. (2025). Financially Motivated Sextortion. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/sextortion/financially-motivated-sextortion

[5] Ray, A., & Henry, N. (2025). Sextortion: A Scoping Review. *Trauma, Violence, & Abuse*, *26*(1), 138-155. https://doi.org/10.1177/15248380241277271

[6] Wolak, J., et al. Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health* 62.1 (2018): 72-79. https://doi.org/10.1016/j.jadohealth.2017.08.014

[7] Freed, D., et al. (2025). Help-seeking and Coping Strategies for Technology-facilitated Abuse Experienced by Youth. *Proc. ACM Hum.-Comput. Interact.* 9, 2, Article CSCW094 (May 2025), 25 pages. https://doi.org/10.1145/3710992

[8] Committee to Evaluate the Supplemental Security Income Disability Program for Children with Mental Disorders; Board on the Health of Select Populations; Board on Children, Youth, and Families; Institute of Medicine; Division of Behavioral and Social Sciences and Education; The National Academies of Sciences, Engineering, and Medicine; Boat TF, Wu JT, editors. Mental Disorders and Disabilities Among Low-Income Children. Washington (DC): National Academies Press (US); 2015 Oct 28. Available from: https://www.ncbi.nlm.nih.gov/books/NBK332882/ doi: 10.17226/21780

[9] Zablotsky, B., Black, L. I., Maenner, M. J., Schieve, L. A., Danielson, M. L., Bitsko, R. H., Blumberg, S. J., Kogan, M. D., & Boyle, C. A. (2019). Prevalence and Trends of Developmental Disabilities among Children in the United States: 2009-2017. *Pediatrics*, *144*(4), e20190811. https://doi.org/10.1542/peds.2019-0811

Definitions:

Gender-based violence. Any harmful threat or act directed at an individual or group based on actual or perceived sex, gender, gender identity, sex characteristics, or sexual orientation.

Sextortion. A non-physical form of coercion where a perpetrator threatens to send out someone's private or sensitive materials or intimate pictures if they do not provide them with more sexual images, sexual favors, or money.

Image-based gender-based violence. The use of synthetic content generated by Artificial Intelligence (AI) and real intimate images distributed without a person's consent.

Impersonation. Using fake social media, false email accounts, etc., to use an individual's name and photo to discredit, expose, or compromise that individual.

Catfishing. A slang term used to describe an individual who lies about their identity, typically on social media, apps, etc., to intentionally deceive, harm, or scam another person.

Non-consensual intimate image sharing. An act of sharing an intimate or sexually explicit image or recording of another person without their consent.

Deepfakes. An image or recording that has been altered or manipulated to misrepresent someone doing or saying something that they never did.

Sexually explicit deepfakes. An image or recording that has been altered or manipulated to misrepresent someone performing a sexual act or saying something of a sexual nature that they never did.

Cyberbullying. The practice of electronic harassment that can occur through a computer or phone.

Financial exploitation. The improper use of a person's funds, property, or resources by another individual. It includes, but is not limited to, fraud, false pretenses, embezzlement, conspiracy, forgery, falsifying records, coerced property transfers, and denial of access to assets, all of which are crimes under the law.

504s. 504 Plans operate under Section 504 of the Rehabilitation Act of 1973, a federal civil rights law focused on nondiscrimination. Section 504 does not create an entitlement to special education. Responsibility instead centers on ensuring equal access to programs and activities offered by schools receiving federal funding. Compliance under Section 504 requires schools to identify barriers created by disability and remove those barriers so students can participate alongside peers. Legal protection does not end at graduation and continues into colleges, universities, and other federally funded institutions.

IEPs. IEPs arise under the Individuals with Disabilities Education Act, a federal special education statute that creates an entitlement to services. IDEA places an affirmative duty on public schools to identify eligible students, evaluate educational needs, and deliver instruction designed around those needs. Access to a Free Appropriate Public Education occurs through individualized planning rather than general adjustments. IDEA defines how instruction must be delivered and where it must occur. Instructional placement centers on participation with nondisabled peers to the maximum extent appropriate, supported by safeguards that regulate how services are provided and reviewed. Key legal obligations under IDEA include:

- Provision of specially designed instruction at no cost to families
- Delivery of related services tied directly to educational benefit
- Education in the least restrictive environment whenever appropriate
- Enforceable procedural protections tied to evaluation, placement, and services

Social Media

YouTube
Video-sharing platform for entertainment, tutorials, and creator content.

TikTok
Short-form video app driven by trends, music, and viral creativity.

Instagram
Visual platform for photos, stories, and curated self-presentation.

Snapchat
Ephemeral messaging app for private, friend-to-friend sharing.

Facebook
Legacy social networks now used more for groups and events.

WhatsApp
Encrypted messaging app for personal and group communication.

X (formerly Twitter)
Microblogging site for real-time conversation and news.

Reddit
Forum-based platform for discussion within topic communities.

Discord
Community platform with voice, text, and video channels by interest.

Pinterest
Visual discovery platform for saving and sharing ideas on style, design, and lifestyle inspiration.

Twitch
Live-streaming platform focused on gaming and creative content.