Exhibit 1

IN THE SUPERIOR COURT OF THE STATE OF DELAWARE

ROSALIND "ROS" DOWEY, Individually and as Administrator of the Estate of M.D.; MARK DOWEY, Individually and as Administrator of the Estate of M.D.; and TRICIA MACIEJEWSKI, Individually and as Administrator of the Estate of L.M.; TAMIA WOODS, Individually and as Administrator of the Estate of J.W.; TIM WOODS, Individually and as Administrator of the Estate of J.W.; SHANNON HEACOCK, Individually and as Administrator of the Estate of E.H.; BRITTNEY BIRD, Individually and as Administrator of the Estate of B.B; and PARKER SIEMS, Individually,-	C.A. No. 25C-12-250 CLS
Plaintiffs,	TRIAL BY JURY DEMANDED
v.	
META PLATFORMS, INC. and INSTAGRAM, LLC,	
Defendants.	

AMENDED COMPLAINT

I. INTRODUCTION

1. Plaintiffs Rosalind "Ros" Dowey, Mark Dowey, ~~and~~ Tricia Maciejewski, Tamia Woods, Tim Woods, Shannon Heacock, Brittney Bird, and Parker Siems bring this action for wrongful death and survivorship against Meta Platforms, Inc. and Instagram, LLC (collectively, "Meta") for the deaths of their children M.D., ~~and~~ L.M., J.W., E.H. and B.B. caused by their use of the Meta products Instagram and Facebook.

2. M.D., ~~and~~ L.M., J.W., E.H., and B.B. all died after being sextorted by predators to whom Meta provided personal data and unfettered access as a matter of design.

3. Lawsuits across the U.S. recently have resulted in the public disclosure of internal Meta studies, reports, emails, and other records that acknowledge Instagram and Facebook design defects and company practices that caused the deaths of ~~M.D. and L.M~~these children~~.~~ and which include:

a. Meta's collection of personal data without informed consent, and its subsequent use of such data in its programming of recommendation products it knew it was operating in a manner that recommended teen Instagram and Facebook users to sextortionists who Meta itself already had identified as predators.

b. Meta's failure to safeguard user privacy, including through its continued sharing of Follower and Following data as among minor users and strangers, even after Meta knew that this engagement-focused product feature was resulting it sextortion related deaths of teen users across the world.

c. Meta's conscious refusal to adopt efficient, available, and "expected" safety features and settings its Meta's safety teams begged the company to implement.

d. Meta's multi year campaign of false and misleading statements designed to convince children and parents that ~~Instagram was~~its products were safe for teens at the same time that internal testing showed that ~~Instagram~~ Meta was matchmaking children to adult predators. Even after Meta claimed to have fixed such defects, its personnel confirmed that the alleged remedies were defective, which information Meta also did not publicly disclose.

e. Meta's design and distribution of broken or ineffective reporting mechanisms and platform rules it never intended to enforce.

f. Meta's choice to allow known criminal misconduct and child exploitation to continue on its platforms for the purpose of safeguarding its engagement metrics.

4. The deaths of M.D., ~~and~~ L.M., J.W., E.H., and B.B. were the foreseeable result of Meta's design decisions and repeated refusals to implement affordable, available, and identified safety features due to Meta's prioritization of engagement over user safety.

5. These lawsuits do not arise from addiction to Meta's social media products. L.M. only had access to Instagram for two days before his death, while M.D. J.W., E.H., and B.B. generally ~~was~~ were dismissive of social media.

6. For these reasons, Plaintiffs bring claims of strict product liability based upon Meta's defective design that renders its Instagram and Facebook products and product features not reasonably safe for ordinary consumers and teens, and for its failure to warn of such defects and dangers, despite its knowledge that such defects and dangers existed and its ability to make its products exponentially safer with negligible increase in production cost.

7. Plaintiffs also bring claims for common law negligence arising from Meta's unreasonably dangerous social media products and Meta's failure to warn of such dangers. Meta knew that Instagram and Facebook ~~was~~ were defective and inherently dangerous and that Meta's design decisions and failures to warn were causing the exact kinds of harm and in the exact ways as what happened to M.D., ~~and~~ L.M., J.W., E.H., and B.B. Meta chose to do nothing for a period of more than five years, during which time M.D., ~~and~~ L.M., J.W., E.H., and B.B. began and/or continued to use Meta's products, and died as a result.

8. Plaintiffs bring claims for negligent, reckless, and/or intentional infliction of emotional distress. Meta engaged in extreme and outrageous conduct with reckless or intentional

disregard of the probability of causing severe emotional distress to parents of the children it targeted, addicted, and exposed to the calculated dangers of its products.

9. Plaintiffs also bring claims for unjust enrichment and invasion of privacy. Meta has benefited unjustly from its tortious conduct and further, has invaded the privacy of plaintiffs and their children through its myriad actions designed to intruded upon consumers' solitude, seclusion, and private affairs. This includes manipulating and exploiting users and exceeding the consent provided, if any, by users and their parents to access personal data and use Meta's products.

II. PARTIES

10. Plaintiff Tricia Maciejewski, mother of L.M., deceased, is a resident of Shippensburg, Pennsylvania. Tricia is serving as the Administrator and Personal Representative of her deceased son's estate. Tricia brings this action on her own behalf and on behalf of her deceased son. Tricia has not entered into a User Agreement or other contractual relationship with Defendants herein in connection with L.M.'s use of their products and expressly disaffirms any and all such agreements into which L.M. may have purported to enter. As such, neither she nor the Estate are bound by any arbitration, forum selection, choice of law, or class action waiver set forth in said User Agreements.

11. Plaintiffs Rosalind "Ros" and Mark Dowey, parents of M.D., deceased, are residences of Dunblane, United Kingdom. Ros and Mark are serving as the Administrators and Personal Representatives of their deceased son's estate. Ros and Mark bring this action on their own behalf and on behalf of their deceased son. Ros and Mark have not entered into a User Agreement or other contractual relationship with Defendants herein in connection with M.D.'s use of their products and expressly disaffirms any and all such agreements into which M.D. may have purported to enter. As such, neither they nor the Estate are bound by any arbitration, forum

selection, choice of law, or class action waiver set forth in said User Agreements.

12. Plaintiffs Tamia and Tim Woods, parents of J.W., are residents of Streetsboro, Ohio. Tamia and Tim are serving as the Administrators and Personal Representatives of their deceased son's estate. Tamia and Tim bring this action on their own behalf and on behalf of their deceased son. Tamia and Tim have not entered into a User Agreement or other contractual relationship with Defendants herein in connection with J.W.'s use of their products and expressly disaffirms any and all such agreements into which J.W. may have purported to enter. As such, neither they nor the Estate are bound by any arbitration, forum selection, choice of law, or class action waiver set forth in said User Agreements.

13. Plaintiff Shannon Heacock, mother of E.H., deceased, is a resident of Glasgow, Kentucky. Shannon is serving as the Administrator and Personal Representative of her deceased son's estate. Shannon brings this action on her own behalf and on behalf of her deceased son. Shannon has not entered into a User Agreement or other contractual relationship with Defendants herein in connection with E.H.'s use of their products and expressly disaffirms any and all such agreements into which E.H. may have purported to enter. As such, neither she nor the Estate are bound by any arbitration, forum selection, choice of law, or class action waiver set forth in said User Agreements.

14. Plaintiffs Brittney Bird and Parker Siems, parents of B.B., Kronenwetter and Wausau, Wisconsin, respectively. Brittney currently is serving as the Administrator and Personal Representative of her deceased son's estate. Brittney and Parker bring this action on their own behalf and on behalf of their deceased son. Brittney and Parker have not entered into a User Agreement or other contractual relationship with Defendants herein in connection with B.B.'s use of their products and expressly disaffirms any and all such agreements into which B.B. may have

purported to enter. As such, neither they nor the Estate are bound by any arbitration, forum selection, choice of law, or class action waiver set forth in said User Agreements

~~12.~~15. Defendant Meta Platforms, Inc. ("Meta Platforms") is a multinational technology conglomerate and is a corporation of the State of Delaware which is authorized and registered to transact business within the State of Delaware and does transact business within the State of Delaware. Its registered agent for service of process within the State of Delaware is Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

~~13.~~16. Meta Platforms' subsidiaries include, but may not be limited to, the entities identified in this section, as well as a dozen others whose identity or involvement is presently unclear.

~~14.~~17. Defendant Instagram, LLC ("Instagram, LLC") is a limited liability company of the State of Delaware which is authorized and registered to transact business within the State of Delaware and does transact business within the State of Delaware. Its registered agent for service of process within the State of Delaware is Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

~~15.~~18. Instagram, LLC launched an app called Instagram in October 2010. On or around April 7, 2012, Meta Platforms purchased Instagram, LLC for over one billion dollars and reincorporated the company in Delaware. Meta Platforms is the sole member of this LLC, whose principal place of business is in Menlo Park, CA.

~~16.~~19. Meta Platforms and Instagram are referred to jointly as "Meta."

III. JURISDICTION AND VENUE

~~17.~~20. This Court has general jurisdiction over this matter because Meta Defendants are incorporated in the State of Deleware.

~~18.~~21. The Meta Defendants Operate Globally as a Common and Inseparable Enterprise

~~19.~~22. Plaintiffs have named the proper defendants in this case as Meta, to the extent it owns and/or operates any entity in or involving the United Kingdom, and operates as a single operating entity with regional contracting arms.

~~20.~~23. Meta may own and/or control corporate subsidiaries in other countries in which its products are available, however, these defendants exert complete and total control over all such entities.

~~21.~~24. Mark Zuckerberg is the CEO of Meta, and has maintained complete authority over Meta and all aspects of Meta and its business from its founding to today.

~~22.~~25. Moreover, in M.D.'s case and others, law enforcement in Scotland could not obtain information relating to M.D. and his use of Instagram from any entity but the U.S. Meta entities. They were required to go through the U.S. Department of Justice to obtain information and evidence from Meta and, likewise, preservation orders had to be sent to Meta in the U.S.

~~23.~~26. The same is true structurally. That is, Meta controls global systems, if any, including but not limited to technologies, processes, guidelines, and other relevant factors.

~~24.~~27. Meta manages, oversees, and otherwise handles law enforcement requests and planning out of its Deleware registered U.S. entities, while employees, irrespective of location and nominal employer entity, utilize shared communication systems and discuss and engage seamlessly on product, marketing, distribution, and other relevant subject matters.

~~25.~~28. On information and belief, Meta plans and launches retail and marketing plans at the U.S. entity level and benefits greatly from its branding as a single product and entity.

~~26.~~29. Meta and, specifically, these defendants are the controlling entities as it relates to M.D. and L.M.'s use of their products and resulting deaths.

IV. ONLINE SEXTORTION AND TEEN SUIDICE

A. Sextortion Has Led to an Epidimic of Suicide Deaths Among Teenage Boys

~~27.~~30. Sextortion is a form of child sexual exploitation where children are threatened or blackmailed, most often with the possibility of sharing with the public a nude or sexual images of them, by a person who demands additional sexual content, sexual activity or money from the child. This crime may happen when a child has shared an image with someone they thought they knew or trusted, but in many cases they are targeted by an individual they met online who obtained a sexual image from the child through deceit, coercion, or some other method. In many cases, the blackmailers may have stolen or taken images of another person and they are communicating through a fake account. The blackmailer may have sent images as well.

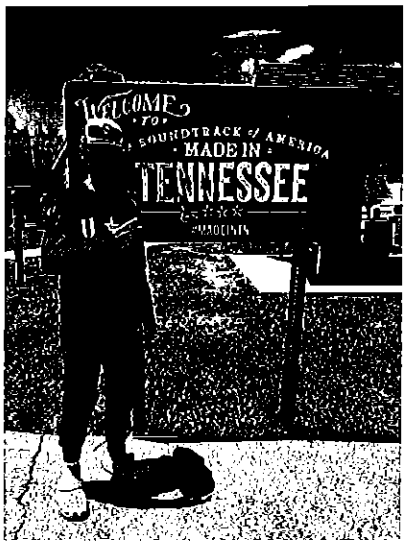
~~28.~~31. According to the FBI, sextortion usually starts when young people believe they are communicating with someone their own age who is interested in a relationship or with someone who is offering something of value. After the criminals have one or more videos or pictures, they threaten to publish that content, or they threaten violence, to get the victim to produce more images. The shame, fear, and confusion children feel when they are caught in this cycle often prevents them from asking for help or reporting the abuse.

~~29.~~32. According to the National Center for Missing and Exploited Children, there has been a 7,200% increase in sextortion attempts in the U.S. between 2021 and 2023 rising to 26,700 in 2024. The FBI also has recently seen an increase in financial sextortion cases targeting minor victims in the U.S. In these cases, the offender receives sexually explicit material from the child and then threatens to release the compromising material unless the victim sends money and/or gift cards. The amount requested varies, and the offender often releases the victim's sexually explicit material regardless of whether or not they receive payment.

~~30.~~33. Teenage boys are the most common targets of sextortion which the FBI relates has resulted in significant number of deaths by suicide. The BBC reported in 2024 that at least 27 boys had died of suicide in the past two years after being sextorted on social media and there have been at least ten additional deaths in 2025.

B. L.M. Died After Being Sextorted on Instagram

L.M. (2011 – 2024)



~~31.~~34. L.M. was born on January 18, 2011.

~~32.~~35. L.M. was passionate about football, baseball, golf, and hunting.

~~33.~~36. He was raised in Cumberland County, Pennsylvania, where hunting is part of the community and where children are taught safe handling of firearms. L.M. took a hunter safety course and passed with flying colors.

~~34.~~37. He also was funny and outgoing. He always knew how to make his parents smile, had endless energy and kindness for those around him, and was the baby and center of his family.

~~35.~~38. L.M.'s parents have always been guarded when it came to screens and devices around their children. They installed passcodes on family televisions to ensure age appropriate shows; prohibited video game consoles in the home, with the exception of a fifteen year old

PlayStation that the boys occasionally could use to play fishing games; and researched every other type of device brought into the home and available parental controls.

~~36.~~39. L.M. has an older brother, B.M.

~~37.~~40. B.M. got his first cell phone at 13, but only because COVID was underway and his parents wanted to make sure that he had a way to stay in contact with his friends. They were not happy about getting him a device, but they understood that there were ways to limit excessive use and safeguard him from harmful online products.

~~38.~~41. At the time, Tricia and her husband used Android devices. But when they began looking for a device for B.M., Apple marketed itself to teens as being easier to use, more intuitive, more accessible, and safe. So they all switched to Apple, and Tricia installed all available parental and family controls on B.M.'s device.

~~39.~~42. This included requiring permission for B.M. to download and use any apps.

~~40.~~43. Tricia said no to social media, then agreed to let B.M. use Instagram when he was 14 or 15. First, she understood that Instagram was the app used by college sports recruiters and B.M.'s high school, making it an important tool in his atheletic career. Second, she looked into Meta's safety representations. She checked Instagram out in the Apple App store and read up on it via publicly available information.

~~41.~~44. Because of Meta's representations, Tricia believed that Instagram was safe for kids as young as 12. Tricia understood that kids could find friends they already knew on Instagram, and never saw anything about how the product would push and recommend strangers to young users and/or share her child's personal information by pushing it out to strangers. In fact, she remembers seeing Meta announcements about how safe its product was for teens in particular; how it was private, and how Meta took extensive steps to keep kids safe on its platform.

~~42.~~45. Tricia was an educator and would have been familiar with Meta in conjunction with its efforts to infiltrate schools. She recalls tech companies like Apple pushing for adoption of iPads for children; convincing adminstrators that those devices were safe. Tricia was involved in some of those discussions, which included the adoption of tech as the newest and best educational tool. It felt like the next and natural step and schools that did not have the newest and best tech products felt like they were behind. During this same time, Instagram also partnered with organizations like Scholastic and the PTA and did so in a manner designed to give its products credibility, and provided assurances that they were safe.

~~43.~~46. According to Meta's own documents, it partnered with organizations like this because they were "trusted, respected organizations" with "significant credibility" that could "be a public validator" for the company and could "get our materials into the hands of parents, grandparents, and educators at scale." Meta wrote, "If you want to connect with parents at scale, you work with the PTA." So that is what it did, and it convinced educators and parents like Tricia that it could be trusted and that its products belonged in schools.

~~44.~~47. Tricia said yes to Instagram for her oldest son because Meta convinced her that it was an age-appropriate product and because Meta had positioned Instagram as something high school athletes needed to connect with recruiters.

~~45.~~48. Even though B.M. had a phone and Instagram, Tricia's youngest child, L.M., did not. Then, when L.M. was 11 there was an active shooter lock down on his second day of school.

~~46.~~49. Tricia worked at the local elementary school, and this was the first year L.M. was not in her line of sight every day. He had moved up to the middle school. When Tricia heard about the incident at his school that day, she was terrified and felt helpless.

~~47.~~50. So the next morning she connected L.M.'s device to a phone line to ensure that he

could use the device anywhere and in case his parents needed to reach him any time of day.

~~48.~~51. Tricia had not planned to provide L.M. with a phone number at age 11. She planned to wait until at least 13. But the tech industry's fear-based narrative about every child needing a device in case of emergency was convincing. Tricia can see *now* that this is not the answer. She knows that schools are equipped to handle active shooter situations and that devices only create more chaos and risk in classrooms; but at the time, it was hard to see past the fear of not being with her son and the convenience of devices the tech industry convinced her were perfectly safe for American children of all ages.

~~49.~~52. Tricia got L.M. an iPhone and, again, installed all available parental controls.

~~50.~~53. She set ground rules, and stuck to them, and everything seemed to be okay.

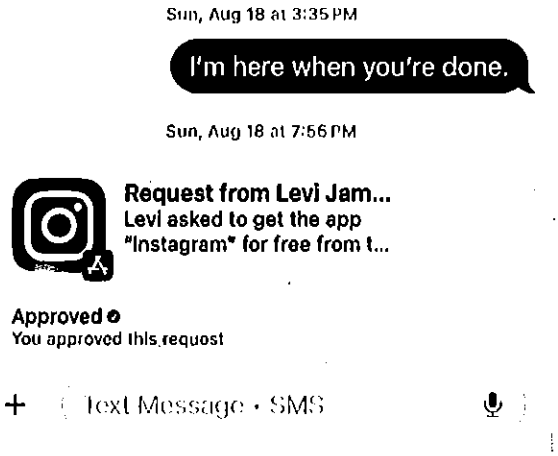
~~51.~~54. Then, L.M. asked for Instagram. He was 13 at the time, and his phone was set up so that he could not get any apps without his mother's express approval.

~~52.~~55. He occasionally would ask for apps and, each time, Tricia would investigate, look up the app, and make a decision based on what she found. More often than not, she said no.

~~53.~~56. But when L.M. asked for Instagram, it was two days before the start of 8th grade. L.M. had spent the day with his best friend riding go-karts, then swimming. Tricia fed they boys then took L.M.'s friend home, and the two of them went for a drive in the mountains with the topless jeep. They got caught in a thunderstorm and laughed the whole drive home.

~~54.~~57. L.M. told his mom, "Mom, I love making memories like this with you."

~~55.~~58. Then when they got home, he jumped into the hammock and Tricia began folding laundry. Then her phone pinged with an app request from her thirteen-year-old son, L.M.



~~56.~~59. Tricia thought about the request. She thought about all the times she said "no" to app requests, and about how Instagram was as safe as it got for teens (according to Meta); how L.M. was into sports like his brother and would need it for recruiting; how good of a kid L.M. was and how responsible he had been with his phone since he got it.

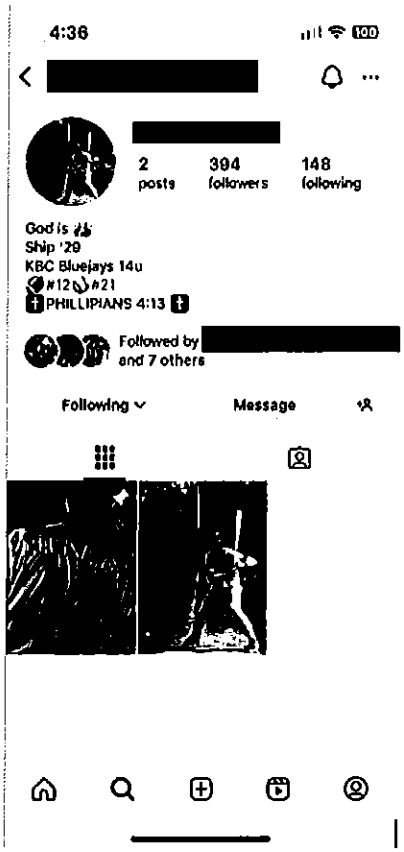
~~57.~~60. Tricia did the calculation in her head and concluded "Meta cares about kid safety."

~~58.~~61. So this time, Tricia said "yes."

~~59.~~62. On August 18, 2024, 13-year-old L.M. started his first Instagram account.

~~60.~~63. By August 20, 2024 – two days later – L.M. was dead.

~~61.~~64. L.M. loved baseball and God, and he made both of those passions clear on his Instagram profile. Somehow, he had hundreds of followers just days after starting his first account.



~~62.~~65. On August 20, 2024, L.M.'s family believed he died of a misfire/hunting accident. He was in the backyard of the family home, which overlooks acres of farmland.

~~63.~~66. Then, days later, law enforcement told them that it was not an accident. They told them that L.M. was the victim of sextortion and Instagram.

~~64.~~67. On the morning of August 20, 2024, Instagram connected L.M. with a predator posing as a young girl, which predator had then been granted instant and unfettered access to 13-year-old L.M.

~~65.~~68. Instagram does this as a matter of design. It pushes the personal information of minor users to adult predators; including accounts where Meta has received multiple reports of predation and where Meta has independent knowledge of the same.

~~66.~~69. Meta targeted L.M. with its Artificial Intelligence (AI) driven user recommendation

tool, affirmatively facilitating and creating connections between him and complete strangers; persons he did not know in real life and would not have met but for the seemingly random connections Meta made. Meta also targeted him with harmful social comparison and social rewards tools and features, including things like the "like" button and social rewards and validation systems, which caused further harm. Meta encouraged L.M. to trust and accept this stranger by design and inclusion because he had no reason to distrust Meta. Meta claimed it was safe and had protections in place, including privacy protections for teen users.

~~67.~~70. In fact, as recently released Meta documents prove, Meta was fully aware of these risks years prior to August 2024. Meta's safety teams had sounded every alarm bell and begged Meta leadership to institute very simple and cost-effective safety features that would have protected young users like, and specifically including, L.M.

~~68.~~71. Meta leadership made a business decision to not fix its defective and/or inherently harmful product features or install the types of safety features its safety team repeatedly proposed.

~~69.~~72. Meta made the connection, and gave this user unfettered access to L.M.

~~70.~~73. At all times relevant, Meta knew that L.M. was a minor yet distributed its defective and inherently dangerous product to him anyway.

~~71.~~74. The predator Instagram pushed to L.M. convinced him that they were a young girl and to send compromising pictures, then threatened to distribute those to his friends and family.

~~72.~~75. The Instagram-enabled-predator demanded that L.M. pay $300. L.M. only had $37.18 in his Greenlight card and some cash on his nightstand. But he could not figure out how to get them the money. The predator told him to get gift cards and set a deadline.

~~73.~~76. The predator told him that if he did not pay, they would send the photos to his friends and family via the very public mechanisms Meta provides.

~~74.~~77. On information and belief, the predator that sextorted L.M. had multiple Instagram accounts. Most Meta predators do; it allows them to keep exploiting children when one account is taken down, establish credibility (for example, by increasing friend counts through a larger network), and continue harassing children who attempt to block them.

~~75.~~78. Meta knows the real age of a predator who extorted L.M. Meta also knows when a user has multiple accounts and often knows when an account is being used to groom or exploit children. Meta obtains independent knowledge of things like age because Meta uses such knowledge for product development and marketing purposes. It then disregards such knowledge as it relates to user safety. It also is likely that this particular predator who sextorted L.M. had been reported to Meta by other users, by law enforcement, and/or by Meta's own employees. Plaintiffs will be entitled to discovery on this issue.

~~76.~~79. Meta's decisions provided this predator with the tools and access needed to exploit and sextort L.M. *years* after Meta had knowledge that its products were causing these exact harms in these exact ways.

~~77.~~80. L.M. felt vulnerable and trapped as the result of his use of Instagram – a product he trusted based on Meta's representations and promises that it was safe and fun.

~~78.~~81. The types of harms L.M. suffered as the result of his Instagram use were not only foreseeable by Meta, they were known to Meta as a design-based risk inherent in its' platforms chosen architecture.

~~79.~~82. What is not yet known and will require discovery is whether L.M. also attempted to report the harms he was suffering to Meta directly, and whether Meta acted on such reports; or if Meta simply ignored those efforts to obtain help, as it reportedly does in a significant number of instances. In this regard, Meta's reporting and response features also are defective, which Meta

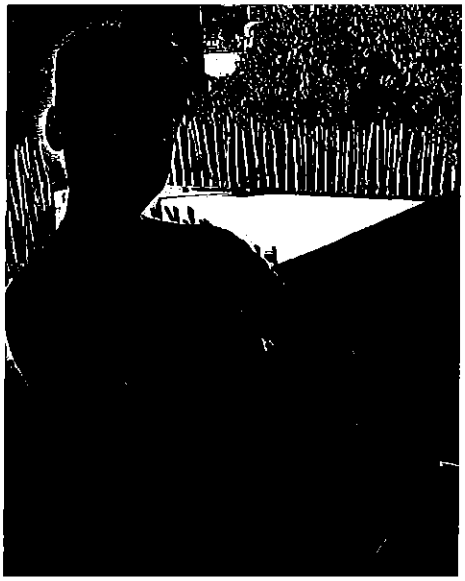
knew, and about which defects it failed to warn consumers

~~80.~~83. On August 20, 2024, L.M. died by a self-inflicted gun shot wound as the result of the harms inflicted on him by Meta and its Instagram product as a matter of product design. His was ruled a homicide.

~~81.~~84. It only took two days after his Instagram use started, and only hours after Meta shared his personal information with a predatory stranger, for these harms to happen.

C. M.D. Died After Being Sextorted on Instagram

M.D. (2007 – 2023)



~~82.~~85. M.D. was born on September 26, 2007.

~~83.~~86. He was clever, funny, and sociable; passionate about his football team and his guitar but preferred to play his guitar in private. M.D. wasn't big on being in the spotlight, though he did perform once at a school event. He was also strong-willed.

~~84.~~87. When M.D. set his mind against something, he stuck to that decision; and likewise, when he set his mind to do something, he did it.

~~85.~~88. M.D. was the peacemaker of his family, and the glue that held it together.

~~86.~~89. M.D. began using Instagram in May 2018, when he was 10 years old. At all times

relevant, Meta knew that M.D. was a minor.

~~87.~~90. He was not particularly attached to his phone and, if anything, was slightly dismissive of social media in general. Instagram was the exception, and his parents understood based on Meta's reputation and representations that Instagram was safe for kids.

~~88.~~91. In fact, they recall Meta's marketing of teen safety features and never saw anything in any of Meta's commercials or elsewhere discussing the risk of adult predators being pushed to or even able to connect with teens. They would not have been okay with the use of Instagram had Meta been honest or had it warned of its defects and inherent dangers.

~~89.~~92. On December 29, 2023, Mark, Ros, and their three sons were watching television together and talked about their plans for the new year. It was a typical, relaxing evening at home. M.D. talked about saving up for a holiday to Marbella that he and his friends were planning that summer and, at about 9:30 pm, he went up to his bedroom for the night

~~90.~~93. Sometime after 9:30 pm, Instagram connected him M.D. to a predator. Meta encouraged M.D. to trust and accept this stranger by design and inclusion because he had no reason to distrust Meta. Meta claimed it was safe and had protections in place, including privacy protections for teen users.

~~91.~~94. Meta made the connection, and gave this predator unfettered access to M.D.

~~92.~~95. Meta knew that he was a minor and distributed its defective and inherently dangerous product to him anyway and did not warn M.D. or his parents about the defects.

~~93.~~96. On December 29, 2023, the predator Instagram pushed to M.D. by design convinced him that they were a young girl and to send compromising pictures, then threatened to distribute those to his friends and family.

~~94.~~97. On information and belief, the predator that sextorted M.D. had multiple Instagram

accounts. It also is likely that this particular predator and/or account had been reported to Meta by other users, by law enforcement, and/or by Meta's own employees. Plaintiffs will be entitled to discovery on this issue.

~~95.~~98. Meta's decisions provided this predator with the tools and access needed to exploit and sextort M.D. *years* after Meta had knowledge that its products were causing these exact harms in these exact ways.

~~96.~~99. Meta targeted M.D. with its Artificial Intelligence (AI) driven user recommendation tool, affirmatively facilitating and creating connections between him and complete strangers; persons he did not know in real life and would not have met but for the seemingly random connections Meta made. Meta also targeted him with harmful social comparison and social rewards tools and features, including things like the "like" button and social rewards and validation systems, which caused further harm.

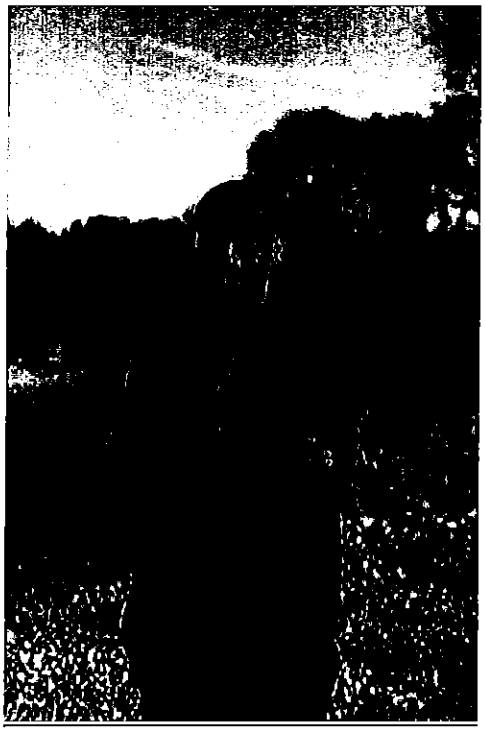
~~97.~~100. M.D. felt vulnerable and trapped as the result of his use of Instagram – a product he trusted based on Meta's representations and promises that it was safe and fun.

~~98.~~101. The types of harms M.D. suffered as the result of his Instagram use were not only foreseeable by Meta, they were known to Meta as a design-based risk inherent in its platforms' chosen architecture.

102. On December 29 or December 30, 2023, M.D. died by suicide as the result of the harms inflicted on him by Meta and its Instagram product as a matter of product design.

D. J.W. Died After Being Sextorted on Instagram

J.W. (2005 – 2022)



103. J.W. was born on July 23, 2005.

104. He was a humble young man, who loved to laugh and joke, and learn things. He was curious and kind. He ran Cross Country, Indoor Track, and Outdoor Track at school, but even when he wasn't doing that, he would run around the neighborhood nonstop. Tamia remembers him running in the middle of winter. He would forget his gloves and come home with his hands so cold that she would rub them warm for him. He was dedicated and never did anything halfway.

105. J.W. began using Instagram in March 2019, when he was 13 years old. He wasn't into the platform very much, or any social media products for that matter. He used Instagram more the last year before he died, but even then, it was not the center of his world.

106. At all times relevant, Meta knew that J.W. was a minor.

107. He set up his Instagram accounting using an incorrect birthday of July 23, 1990.

However, his mother had parental controls on his phone and has him listed in her Apple family account as a child. More importantly, however, Meta utilizes a proprietary algorithm through which it estimates the age of each user and would have estimated J.W.'s age and determined that he was a minor and not a twenty-nine-year-old adult.

108. Among the signals Meta would have used to confirm his real age are things like the fact that his friend group was primarily minors, his photos, his activities, and the school he attended. Meta has gone to extensive efforts to infer school affiliations using complex data mapping techniques. In short, irrespective of what age J.W. input when he opened his account, Meta knew he was a minor and would have utilized that information for purposes such as advertising and product development, while ignoring it for purposes of safety.

109. J.W. parents had parental control on his device. They were careful with his device and app usage and checked in with him often.

110. Meta represented repeatedly that its Instagram product was safe for teens, and Tamia and J.W. would never have allowed their son to use it had Meta told the truth.

111. On November 18, 2022, Meta connected J.W. to an adult user who was preying on U.S. teens via the tools and accounts Meta provided.

112. Meta encouraged J.W. to trust and accept this stranger by design and including because he had no reason to distrust Meta. Meta claimed it was safe and had protections in place, including privacy protections for teen users. In fact, by this time, Meta had assured J.W. and minors like him that unconnected adults could not even message them.

113. Meta made the connection, and gave this predator unfettered access to J.W.

114. Meta knew that he was a minor and distributed its defective and inherently dangerous product to him anyway and did not warn J.W. or his parents about the defects.

115. On November 18, 2022, the predator Instagram pushed to J.W. by design convinced him that they were a young girl and to send compromising pictures, then threatened to distribute those to his friends and family.

116. On information and belief, the predator that sextorted J.W. had multiple Instagram accounts. It also is likely that this particular predator and/or account had been reported to Meta by other users, by law enforcement, and/or by Meta's own employees. Plaintiffs will be entitled to discovery on this issue.

117. In fact, with the information Tamia and Tim provided to law enforcement, they believe that they were able to find at least 50 other sextortion incidents in Ohio alone and linked to the same CashApp account that was used to sextort J.W. On information and belief, these schemes almost always involve Meta platforms, at least the successful ones—including because Meta provides predators with more personal information about minor users than other platforms.

118. The night J.W. died – November 19, 2022 – law enforcement (Internet Crimes Against Children (ICAC)) contacted Meta to inform them about the predatory Instagram accounts that had been interacting with J.W. According to ICAC, Meta took down all of the predator's pages and associated pages without requiring a subpoena. ICAC said that this was very unusual, as Meta typically would not take down accounts like this – even once it had notice – and unless a subpoena was issued.

119. Notably, Plaintiffs' counsel in this case also filed and served a significantly detailed complaint on Meta on November 15 or 16, 2022 – just three days before J.W.'s death – detailing Meta's failure to act upon notice of predatory accounts, specifically in the context of sextortion, and how those failures were causing irreparable harms to countless U.S. children.

120. A true and correct copy of that Complaint is attached hereto as **Exhibit A**.[1]

121. Meta had notice of every allegation contained in that Complaint prior to J.W.'s death, and in fact, prior to the death of all of the children named in this amended complaint.

122. Meta made business decisions to prioritize engagement over the health and safety of its young users, like and specifically, J.W.

123. J.W. did not consent to Meta's provision of his personal information to other users. None of Meta's minor users knowingly consent or have opportunity to provide informed consent to these design decisions and violating practices, which Meta employs for purpose of increased engagement, despite knowing the serious safety risks it creates for young users.

124. Meta's decisions provided this predator with the tools and access needed to exploit and sextort J.W. *years* after Meta had knowledge that its products were causing these exact harms in these exact ways.

125. Meta targeted J.W. with its Artificial Intelligence (AI) driven user recommendation tool, affirmatively facilitating and creating connections between him and complete strangers; persons he did not know in real life and would not have met but for the seemingly random connections Meta made. Meta also targeted him with harmful social comparison and social rewards tools and features, including things like the "like" button and social rewards and validation systems, which caused further harm.

126. J.W. felt vulnerable and trapped as the result of his use of Instagram – a product he trusted based on Meta's representations and promises that it was safe and fun.

127. The types of harms J.W. suffered as the result of his Instagram use were not only foreseeable by Meta, they were known to Meta as a design-based risk inherent in its platforms'

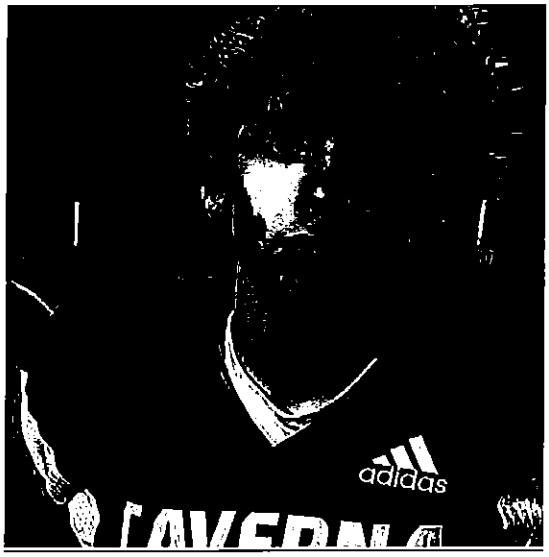
[1] The *A.C. v. Meta Platforms, et. al.* matter referenced in the attached exhibit was voluntarily dismissed in February 2023 and immediately refiled in the Northern District of California. That lawsuit is pending as of this filing.

chosen architecture.

128. On November 19, 2022, J.W. died by suicide as the result of the harms inflicted on him by Meta and its Instagram product as a matter of product design.

E. E.H. Died After Being Sextorted on Facebook

E.H. (2008 – 2025)



129. E.H. was born on November 8, 2008.

130. Shannon referred to E.H. as her "tornado." He was a prankster and brought joy to those around him. He was the kid who lit up rooms and always cheered on friends and teammates, no matter the score. He was happy just to be himself.

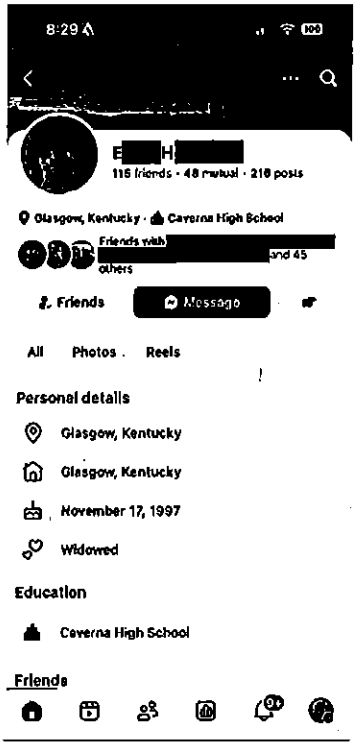
131. Shannon believes that E.H. was 12 or 13 when he started using Meta's Facebook product. He wasn't really into social media, and his parents understood based on Meta's representations and reputation that Facebook was safe for teens.

132. In fact, it was the platform their children's schools used for sports teams.

133. They would not have been okay with his use of Facebook had Meta been honest or had it warned of its defects and inherent dangers.

134. Meta also knew, at all times, that E.H. was a minor.

135. For example, while E.H. put his date of birth at November 1997 on his Facebook account, Meta knew that he attended Caverna High School.



136. It knew for multiple reasons, including because E.H. told Meta and because Meta utilizes complex data mapping techniques so that it can ascertain the school each of its minor users attends. Meta documents recently made public in other litigation include statements such as,

a. "it is essential that we correctly identify the school a given teen is attending"

b. "we plan to embed each teen as a data point and each school as a multidimensional gaussian" which "will allow us to directly derive the probability of attending any given school"

c. acknowledging the "FB [Facebook] ML [machine learning] school inference model"

137. Meta uses similar proprietary technologies and signaling to ascertain not just which school a minor attends, but their estimated age – which knowledge Meta uses for purposes of advertising and product development, just not safety.

138. For these reasons, Meta knew E.H.'s age at all times. It knew he was vulnerable, and not of legal age to consent to any contractual terms Meta attempted to impose. It took his personal data and shared that data with adult strangers regardless.

139. On February 28, 2025, Shannon picked her son up at school in a new Jeep. He was getting ready to get his driver's license, and she told him that the Jeep would be his car when he did. E.H. was ecstatic. They drove away from the school, and he held her hand as they siwitched gears so that he could learn how to drive a 5-speed. They went to get his cair cut, and picked up some flowers for his favorite teacher before heading home for the night.

140. By 11:30 p.m. that evening, however, E.H. was dead.

141. Law enforcement still has E.H.'s devices, and his parents have not been able to learn much about what happened; except that a predator found E.H. online.

142. Shannon currently does not know for certain which platform the predator first used to contact her son, and discovery will be needed to ascertain whether and at what point the two connected or Meta connected them on Facebook.

143. Shannon does, however, allege that the predator created explicit, AI-generated images of E.H., then used those images to threaten and extort him – including and importantly, on the basis of private information Meta shared with the predator about E.H.

144. Again, E.H.'s parents cannot yet be certain where the contact first started, or whether Meta pushed E.H.'s data to the predator in the first instance. But what they found out just one month prior to the filing of this Amended Complaint was that Meta provided the predator with

access to E.H.'s Facebook "Friend" data, which data the predator was then able to use as lethal leverage.

145. Meta claimed it was safe and had protections in place, including privacy protections for teen users. Yet it provided access to E.H.'s data to an adult predator.

146. Meta gave this predator unfettered access to E.H.

147. Meta knew that he was a minor and distributed its defective and inherently dangerous product to him anyway and did not warn E.H. or his parents about the defects.

148. The predator Meta either pushed to E.H. by design or simply provided with access to E.H. by design demanded $3,000. E.H. sent what he had, which was $50. The predator used E.H.'s Facebook "Friends" data to convince him that the images would be sent to everyone he knew. The incident lasted roughly 20 minutes – during which E.H. received over 150 messages.

149. On information and belief, the predator that sextorted M.D. had multiple Facebook accounts. It also is likely that this particular predator and/or account had been reported to Meta by other users, by law enforcement, and/or by Meta's own employees. Plaintiffs will be entitled to discovery on this issue.

150. Meta's decisions provided this predator with the tools and access needed to exploit and sextort E.H. *years* after Meta had knowledge that its products were causing these exact harms in these exact ways.

151. Meta targeted E.H. with its Artificial Intelligence (AI) driven user recommendation tool, affirmatively facilitating and creating connections between him and complete strangers; persons he did not know in real life and would not have met but for the seemingly random connections Meta made. Meta also targeted him with harmful social comparison and social rewards tools and features, including things like the "like" button and social rewards and validation

systems, which caused further harm.

152. E.H. felt vulnerable and trapped as the result of his use of Facebook – a product he trusted based on Meta's representations and promises that it was safe and fun.

153. The types of harms E.H. suffered as the result of his Facebook use were not only foreseeable by Meta, they were known to Meta as a design-based risk inherent in its platforms' chosen architecture.

154. On February 28, 2025, E.H. died by suicide as the result of the harms inflicted on him by Meta and its Facebook product as a matter of product design.

F. B.B. Died After Being Sextorted on Facebook

B.B. (2009 – 2025)

155. B.B. was born on September 22, 2009.

156. He was a straight A student. He was loving, responsible, and played multiple sports.

157. B.B.'s parents had an exceptional co-parenting relationship, which included B.B.'s stepparents. They spent summers together as one family at B.B.'s baseball tournaments. They encouraged honest and open communication and remained engaged and supportive throughout

B.B.'s teen years.

158. B.B. received his first cell phone as a birthday gift when he turned 12.

159. His father employed every restriction of which he was aware. This included rules around usage, for example, the phone had to be put up by 10 pm each night. It also included rigorous, device-based parental controls. For example, his father would get notifications anytime B.B. wanted a new app. He would look at what was being requested and make what he believed to be an informed decision.

160. B.B.'s parents relied on what companies like Meta told them about their products, and how these products were described and reviewed in app stores.

161. B.B.'s parents also said no to social media of any sort until he was thirteen and a half. Then they talked about each app, and why he believed he needed it. They also required him to add or connect with them on these apps, so that they could see what he was posting and doing generally online.

162. B.B. is believed to have started using Facebook when he was 14.

163. The parental controls on his device had started to become more of a problem than helpful. For example, if he was out, he couldn't call them to check in past 11 pm. They also seemed to stop notifying about new apps after he turned 14. So ultimately, they stopped using the parental controls and opted for ongoing discussions, occasional phone checks, and similar efforts.

164. He did not ask his parents' permission for Facebook, but they were familiar with the platform and understood that it was safe. There was no sense of danger once they knew he had a Facebook account. After all, it was the platform used for sports and at school. It was the platform used to keep in touch with friends and family.

165. Meta was marketing its products to schools, convincing teachers and parents that its

products were essential tools to stay connected and communicate. What Meta never told the world was that it's platforms – including Facebook – were uniquely dangerous for young users because of the design decisions Meta was making.

166. This includes pushing out minor user data to unconnected adult accounts; providing information and access to predatory users via school websites and the appearance of safety; defaulting and encouraging children into low privacy and public settings that are designed to increase Meta's engagement but at the expense of safety; and publicizing the Friend and Follower and Following data of minors to complete strangers.

167. On information and belief, B.B. would not have been interested in Facebook but for the fact that his sports teams and school used it. Whie Meta targeted schools and school-aged children because it determined that they promised the most in terms of value for Meta. The following are just a few examples from now public Meta documents discussing this point,

a. "Tweens and young teens are Facebook's best opportunity to win future generations of people."

b. "Tweens (approximately age 10 to 12) are special. People who join[] Facebook as tweens have the highest long-term retention out of all age groups."

c. "We have definitively established tweens as the highest retention age group in the United States."

168. Like many kids his age, B.B. thought of Facebook as a platform for older people. He had maybe a dozen Friends on his account. But it was also something he felt he needed because of its prevalence among school sports.

169. At all times relevant, Meta knew that B.B. was a minor.

170. On the night of March 5, 2025, Meta connected B.B. to an unconnected adult

stranger. Brittney and Parker do not yet know whether Meta made the recommendation, or if the predator found B.B. through his school sports websites, as predators are doing with countless children in the U.S. – finding athletes and other teens engaged in school activities via the Facebook and Instagram accounts in use and popularized by their schools.

171. What they do know is that, like most teen boys, B.B. did not use Facebook much. It was not the primary app he used to communicate with friends. But when a Facebook user posing as a cute girl reached out to him on Facebook, he responded.

172. Meta encouraged B.B. to trust and accept this stranger by design and including because he had no reason to distrust Meta. Meta claimed it was safe and had protections in place, including privacy protections for teen users.

173. Meta made the connection, and gave this predator unfettered access to B.B.

174. Meta knew that he was a minor and distributed its defective and inherently dangerous product to him anyway and did not warn B.B. or his parents about the defects.

175. The predator Meta pushed to B.B. convinced him that they were a young girl and to send compromising pictures, then threatened to distribute those to his friends and family.

176. On information and belief, the predator that sextorted B.B. had multiple Meta accounts. It also is possible that this particular predator and/or account had been reported to Meta by other users, by law enforcement, and/or by Meta's own employees. Plaintiffs will be entitled to discovery on this issue.

177. Meta's decisions provided this predator with the tools and access needed to exploit and sextort B.B. *years* after Meta had knowledge that its products were causing these exact harms in these exact ways.

178. Meta targeted B.B. with its Artificial Intelligence (AI) driven user recommendation

tool, affirmatively facilitating and creating connections between him and complete strangers; persons he did not know in real life and would not have met but for the seemingly random connections Meta made.

179. Meta further shared B.B.'s Friend information with this predator, which the predator then used to contact B.B.'s stepfather, Luke, on Meta platforms and to prove that he could. Specifically, the predator messaged Luke then recalled the messages, and showed B.B. that he had.

180. Only Luke did not see the message or even the recall prior to B.B.'s death. It was a few weeks later when law enforcement asked him to check his account. Luke did but saw no evidence of such messaging on his phone. So he checked Facebook via his laptop, which is when he saw that the message had been sent and then recalled, the notification for which Meta had put into Luke's Spam folder.

181. By then, it was several weeks too late.

182. Meta knew or had reason to know that the predator was not connected to this family and connected him to B.B. anyway and for engagement's sake.

183. B.B. felt vulnerable and trapped as the result of his use of Facebook – a product he trusted based on Meta's representations and promises that it was safe and fun.

184. The types of harms B.B. suffered as the result of his Facebook use were not only foreseeable by Meta, they were known to Meta as a design-based risk inherent in its platforms' chosen architecture.

185. On March 5, 2025, B.B. died by suicide as the result of the harms inflicted on him by Meta and its Facebook product as a matter of product design.

186. On information and belief, law enforcement notified Meta quickly, and yet, Meta allowed that same account to continue engaging on its platform for at least two more weeks.

~~99.~~ But also, after B.B.'s death and after his parents began speaking out to let other kids know about the sextortion schemes running rampant on Instagram and Facebook, nine different families reached out to let them know that their children had also been sextorted. More to the point, they said that if B.B.'s parents had not spoken out and let the other teens know what was happening and that it would be okay, those teens might not still be here.

187.

V. META KNOWINLY FACILITES ONLINE SEXTORTION OF VULNERABLE TEENS

A. Meta Is Involved In More Sextortion Related Deaths Than Any Other App

~~100.~~188. On information and belief, from 2008 to 2012, Meta's Facebook product was one of the most common vectors that online sextortion criminals used to target their victims. Facebook's features made it the most accessible platform for blackmailers to quickly obtain personal information and initiate a successful sextortion attack.

~~101.~~189. On October 10, 2012, fifteen year old Amanda Todd died in connection with sextortion harms as the result of these defects and dangers. *See Carol Todd et. al. v. Meta Platforms, Inc. et al.*, L.A. Sup. Ct., Case No. 24SMCV04957 (filed Oct. 10, 2024), ¶¶ 115-151.

~~102.~~190. Currently, Meta's Instagram product "is the most common vector that sextortion criminals use to target their victims," and including because "Instagram's design and features make it the most accessible platform for blackmailers to quickly attain personal information about the victim to initiate a successful sextortion attack."[2]

~~103.~~191. This is not a coincidence or an accident. When a specific type of harm proliferates on one similarly situated platform out of many, the difference is by design.

[2] NCRI, A Digital Pandemic: Uncoverying the Rule of 'Yahoo Boys' in the Surge of Social Media-Enabled Financial Sextortion Targeting Minors, January 30, 2024, p. 5. Attached hereto as **Exhibit ~~B~~A**.

B. Meta Facilitates Sextortion Through Facebook and Instagram's AI-Driven Recommendation Systems

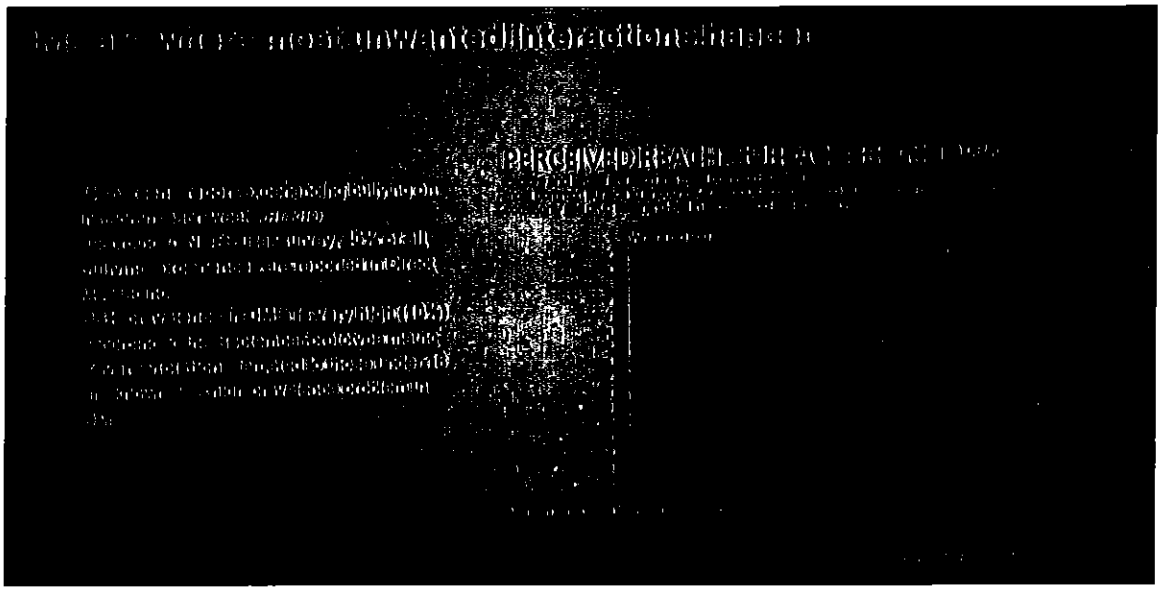
~~104.~~192. Recently unsealed documents establish that Meta directs children to predators and predators to children by design.

~~105.~~193. Instagram has a feature called "Accounts You May Follow," through which the Instagram product recommends accounts to a user, the purpose of which includes increasing engagement on the Platform. Meta conducted studies examining and confirming things such as increased engagement and long-term retention based on its ability to make and maximize such connections during "onboarding" (when a user first starts using its product) and at other times.

~~106.~~194. At the same time, Meta knew that its design and programming decisions specific to this feature were inherently dangerous for minor users, and were causing incredible harms.

~~107.~~195. An internal Meta analysis from 2019 estimated that there were 3.5 million profiles "conducting Inappropriate Interactions with Children" (also referred to internally at Meta as "IIC") over Instagram's Direct Message ("DM") feature.

~~108.~~196. Meta confirmed that its DM feature is "where most unwanted interactions happen," but did not warn the public or take steps to install safety features for minor users.



~~109.~~197. According to Meta documents, the problem was just as bad on its Facebook product.

~~110.~~198. Specifically, Facebook has an analogous account recommendation feature called "People You May Know" and Meta knew that, at least through the end of 2023, "we were recommending minors to potentially suspicious adults and vice versa in PYMK," and that this feature "was responsible for 80% of violating adult/minor connections."

199. Another internal Meta document included employee discussions about this feature. One employee wrote that they had "been collecting instances of friending contributing to harms. The most interesting ones I had found were: … IIC [Inappropriate Interactions with Children]/Grooming – In the past, PYMK contributed up to 75% of all inappropriate adult-minor contact." Another Meta employee responded, "how on earth have we not just turned off PYMK between adults and children?"

~~111.~~200. Likewise and according to Meta's own estimates, in 2023, Instagram's Accounts You May Follow tool recommended to adult groomers "nearly 2 million minors in the last 3 months"—and "22% of those recommendations resulted in a follow request."

~~112.~~201. The situation was just as bad in the reverse.

~~113.~~202. According to an internal audit in 2022, Accounts You May Follow recommended 1.4 million potential IIC violators to teenage users in a single day.

~~114.~~203. Short of actually fixing these known defects in its account recommendation systems, Meta had a duty to warn the public about them.

~~115.~~204. Meta did not warn the public, but instead, repeatedly represented that its Facebook and Instagram products were safe for minors.

C. Meta Knew of Safety Features That Would Prevent Sextortion Prior to M.D., ~~and~~ L.M., J.W., E.H., and B.B.'s Deaths

~~116.~~205. Even assuming Meta did not have a duty to stop programming its AI-driven recommendation systems in a predatory manner, it still could have taken multiple steps to make its products less dangerous for young users by design.

~~117.~~206. One such step would have been to simply stop sharing personal information of its users (particularly minors who did not provide informed consent, or any consent at all) with strangers, including but not limited to user Friend, Follower, and Following data – a product feature Meta knows to be a critical driver in sextortion related deaths.

~~118.~~207. The Contagion Research Institute report attached at **Exhibit B~~A~~** explains why this feature and setting are so dangerous in the context of Instagram,

> The moment an Instagram user accepts the follow request of a scam account, their follower/following list is compromised. This gives criminals easy access to the target's followers and following lists to use as blackmail, threatening to send the compromising photos to all these acquaintances. With Instagram's current configuration, users have no way to protect themselves against their followers and following lists being copied the instant they accept a follow request. …
>
> Instagram can mitigate a vast majority of financial sextortion cases by hiding minors' Followers and Following lists on their platform by default, and by giving all users the option to make these lists private. This setting should be decoupled from the setting to make your Instagram photos public or private.

~~119.~~208. On information and belief, the same types of considerations apply to Facebook; namely, Meta's choice to share private information of known minor users with known, unconnected adult users. And Meta's choice in this regard is engagement driven. That is, sharing the Friend, Follower, and Following data of its minor users increases engagement across the platform.

~~120.~~209. Meta could also have taken the simple and logical step of defaulting teen accounts to the highest privacy settings, which would have prevented strangers from being able to initiate inappropriate interactions with children to whom they were not connected.

210. Meta not only knew that it could implement such a safety feature with ease, but its safety teams urged leadership to do so for years and to prevent the precise harms at issue.

211. For example, in 2009, Facebook's founding engineer sent Mark Zuckerberg and Chris Cox an email proposing parental supervision tools. "I would like to see us add an opt-in feature, which would allow a Facebook user (child) to designate another user (the parent) to have certain auditing rights and limiting controls over the child account," he wrote.

212. "The dynamic that this creates is to give parents an opportunity to act as parents on Facebook as they would in other dimensions of their children's lives … which I believe is the only scalable and effective way to address the issues of minors on Facebook."

213. In reply, Chris Cox (who became Meta's Chief Product Officer) responded that this "doesn't immediately strike me as high-leverage as much as nice to have" and "seems like a bunch of work for things that the parent could do manually.".

214. Meta ultimately did not make parental controls of any sort available to Facebook users until 2023—fully 14 years later—and then, it purposefully created controls that were difficult to find, hard to use, or ineffective. For example, Meta knows that only 0.15% of Youth users are enrolled in theseparental supervision tools—meaning, 99.85% are not. And Meta knows why that is the case, it simply does not want to fix things because safety by design is not as profitable

as engagement first.

~~121.~~

~~122.~~215. Then, in~~For example, in~~ August 2018 – four years before the first death at issue in this Amended Complaint and a full six and a half ~~five~~ years before ~~M~~the most recent death at issue in this Amended Complaint ~~.D.'s death and six years before L.M.'s death~~ – Guy Rosen (Meta's Chief Information Security Officer) emailed Adam Mosseri (Instagram's CEO) naming the problem, which was the same across both of Meta's platforms:

> someone looks me up on Instagram/Facebook because I'm a cute girl, sends me a message (or even a friend request) and we start messaging. That is where all the bad stuff happens (From the "less bad" tier 2 sexual harassment like dudes sending dick pics to everyone; to the tier 1 cases where they end up doing horrible damage.

~~123.~~216. Two months later, *The Atlantic* published an article titled "Instagram Has a Massive Harassment Problem," featuring an image of the Instagram brand in a Dumpster fire. This article discussed the experiences of two 14-year-olds who described receiving expletive-laden comments about their appearance and death threats on Instagram.

~~124.~~217. Meta knew about this safety issue, yet waited months to even begin to study it.

~~125.~~218. Then, in the fall of 2019, Meta designed a research plan internally acknowledging that its existing "privacy" setting on Instagram was, at best, a misnomer—and that "private" accounts could receive a heavy volume of unwanted interactions from strangers, through mentions, tags, and most importantly direct messages.

~~126.~~219. Meta conducted a series of hour-long interviews in Los Angeles with Instagram users, which qualitative research revealed that "participants were most sensitive to unwanted contact and interaction" on Instagram, including "[u]nwanted messages that were sexual in nature," which "were particularly upsetting."

~~127.~~220. Moreover, participants were clear on a solution: "[A]lmost all participants thought that younger users and new users should be defaulted to private" settings.

~~128.~~221. Based on this feedback, the Meta researcher in charge of the 2019 study made two recommendations to leadership: "default[] all teen accounts to private mode" and, "for private mode defaults, limit tagging, mentioning, and group DMs to connected accounts."

~~129.~~222. Meta had a knowledge, evidence, and a recommendation for a simple safety feature. It could have implemented the recommended changes as needed to meet user expectations, and it should have warned the public that Instagram's existing private mode was less protective than they understood it to be. But Meta did neither of these things. Instead, it continued to launch commericals lauding its product as fun and safe, continued to label its products as safe for minors, and continued to represent to families across the world that it prioritized child safety and could be trusted.

~~130.~~223. In March 2020, Meta researchers embarked on an investigation into what they called "Smart Defaults"—"a safer account model for teens" that would "[p]rotect teens from unwanted DMs" and "additional interaction[s]" in order "to keep them safe." In line with Meta's 2019 interviews, this research acknowledged that privacy settings for "mentions and tags are expected" and that failing to make this change would "not match users expectations." The research proposed the option of "default[ing] all new teens into private," which it acknowledged would "keep more people safe from unwanted DMs, tags, and mentions." But at the same time, it outlined the option of "upsell[ing]" teens into an "opt-in" private experience, as that would present "less risk to engagement metrics."

~~131.~~224. Instead of following the safety recommendations of its research team, Meta continued to focus on its bottom line. Rather than working with its engineering team to implement

these common sense changes to protect teen Instagram users from predatory adults, Meta brought in the growth team, to ensure its continued prioritization of engagement over safety. Meta's growth team determined that a true private-by-default would result in a loss of 1.5 million monthly active teens a year. It wrote, "Your data pretty succinctly shows that taking away unwanted interactions via private default settings is likely to lead to a potentially untenable problem with engagement and growth."

~~132.~~ In April 2020, Meta leadership informed the well-being researchers that "We will not create any new default interaction settings for private accounts." Appaulingly, Meta leadership instructed the researchers to gin up a rationalization for the decision—"give us a story that frames our decision that we've already made" by "fram[ing]" this as a tradeoff between "safety vs value."

225. When one Meta researcher asked: "I[s]nt safety the whole point of this team?" another responded, "The point of this team is to prevent another Atlantic article about how shitty instagram is."

~~133.~~226. Despite believing that Meta should "man up and default people," Meta researchers obliged their superiors and endorsed the idea "that we keep the current default interaction settings as-is" – despite knowledge of the terrible harms happening to minor users.

~~134.~~ Meta knew that placing teens into a default-private setting would have eliminated 5.4 million unwanted interactions a day over Instagram direct message alone—including interactions like the ones that resulted in the deaths of M.D., ~~and~~ L.M., and T.W. *years* after Meta researchers had identified and proposed a simple safety feature to prevent such harms. Plaintiffs do not have the precise number as it relates to Facebook, but on information and belief, the impact on safety for minor uses would have been comparable.

D. Meta Consciously Prioritized Profit Over Protecting Vulnerable Teen Users From Sexploitation

~~135.~~227. Within Meta, the public safety imperative of implementing Private by Default to protect children from adult predators was subordinated to Meta's economic interest in maintaining user engagement and the resulting profits.

228. According to Meta's documents, users who join Facebook as 13-year-olds "have an LTV [lifetime value] of approximately $350, higher than all other teen ages (13-18), due to their very high long-term retention." Moreover, "[t]he difference in long term retention can be dramatic, with the people who signed up for Facebook when they were young teens being 100% higher." Teenage users presented another advantage for Meta: they could serve as gateways into the "household ecosystem," including pre-teen siblings. According to one Instagram researcher: "teens are often the ones that other members of the household learn about not only Instagram, but social media in general through."

229. For these reasons, Meta targeted and focused on children like and specifically including M.D., L.M., J.W., E.H., and B.B

230. It set out to "acquire teens as young as possible."

231. For Meta, this very specifically meant NOT designing with safety in mind.

232. For example, when Meta was considering basic types of design-based safety features that could have prevented the tragedies at issue in this Amended Complaint, instead of doing what it had promised consumers and what would have kept kids safer, it brought in its growth team to assess the economics.

~~136.~~233. Meta's growth team was asked to examine "the growth and engagement knock-on effects" of rolling out such a feature, including potential "friending losses" and "engagement declines." And in August 2020, Meta determined that Private by Default would result

in a "2.2% hit to US DAU" and a "2.2% hit to global for teens"—"that is HUGE."

~~137.~~234. Instituting this simple safety feature would have saved millions of children from the sexual abuses occuring on Instagram and Facebook as a matter of design. While Meta was focused solely on whether kids would meet fewer people and engage less as a result.

~~138.~~235. As such, in August 2020, Meta once again failed to implement available safety features that would have mitigated the harms Meta itself was causing as a matter of design.

~~139.~~236. Meta's policy, legal, communications, privacy, and well-being teams all recommended that private-by-default should "Launch Now," observing that this "will increase teen safety" and is "in-line with teen user expectations," "parent expectations," and "regulator expectations."

~~140.~~237. While Meta's growth team recommended "Don't Launch (Now)," noting a likely impact of negative "2.2% topline teen DAP in 5 years."

~~141.~~238. So this critical safety feature was "scrapped due to growth concerns."

~~142.~~239. In March 2021, the discussion was revived once again and, on March 16, 2021, Meta publicly announced that it would be "restricting DMs between teens and adults they don't follow."

~~143.~~240. Meta represented that, with this change, "when an adult tries to message a teen who doesn't follow them, they receive a notification that DM'ing them isn't an option."

~~144.~~241. Not surprisingly, however, there were some significant problems—beyond the fact that Meta's year-long delay had already facilitated 1.9 billion (= 5.4 million x 365) unwanted interactions between adults and minors on Instagram.

~~145.~~242. Among the most significant of those problems was the fact that private by default was supposed to be for all users and, what Meta launched instead "was for new users under

the age of 16"—not existing teen users, new 17- or 18-year old users, or new teen users who lied about their birthday.

~~146.~~243. Some of the children at issue in this Amended Complaint were ~~L.M. was~~ not yet using ~~Instagram~~ Meta's products when Meta made these representations; however, ~~M.D. was~~some were. While all of the parents at issue, ~~He was 13 or 14 when these features launched and his parents~~ would reasonably have understood that Meta was applying ~~these~~ its privacy settings to their children ~~him~~ when Meta was not.

~~147.~~244. Further, Meta's settings were not working even for the smaller subset of users to whom they were applied. Meta knew that its safety settings were defective, including because of its own internal surveys. This included findings after launch that 13% of 13- to 15-years-old were receiving unwanted sexual advances on Instagram, overwhelmingly from strangers. A Meta employee observed, "they are experiencing these issues…facilitated by the product design of Instagram."

~~148.~~245. But also, what launched wasn't actually a "true default setting." Meta was misrepresenting this point, as explained by Instagram's former Head of Safety and Well-Being, "if you said to somebody, oh, this is a account that is private by default, I think an assumption would be, I sign up, I'm a teenager on the platform, my account is private. I will go into settings and change that to be a public account if I want to." Instead, Meta launched a "default preselected option on a screen"—meaning, new users who self-identified as 16-or-under would "get a screen asking me if want to have a public account or a private account, and the private option is selected."

~~149.~~246. Meta's public announcements indicated that adults would not be able to DM minors with a private account, but this belied the spotty execution of its tool. In 2021, Meta learned of several sextortion related incidents occurring in connection with these known defects and lack

of safety features during. The following are just two of those:

a. On October 17, 2021, 15-year-old Braden Markus was the victim of Instagram sextortion. Braden was studying for his driver's ed test when Meta provided his private information to a predator. Twenty-seven minutes later, Braden died. *See Carol Todd et. al. v. Meta Platforms, Inc. et al.*, L.A. Sup. Ct., Case No. 24SMCV04957 (filed Oct. 10, 2024).

b. On December 4, 2021, 16-year-old Carter Bremseth was the victim of Instagram sextortion. Like Braden, Carter was in the process of studying for his driver's ed exam when Meta provided his private information to a predator. Carter died on December 5, 2021. *See Jaime Bremseth et. al. v. Meta Platforms, Inc. et al.*, L.A. Sup. Ct., Case No. 24SMCV03932 (filed August18, 2025).

~~150.~~247. A year later, in February 2022, Meta determined that teens were *still* "receiving DM requests from unconnected adults, breaking [the] public commitment that we made." Indeed, fully "50% of message requests" to teen users were still coming from adults.

~~151.~~248. Taken together, this unfettered acess and resulting, unwanted Direct Message requests remained a serious risk issue for teens more than a year after Meta's "private by default" announcement, with Meta conceding (internally, never externally) that "there have been many gaps in fulfilling our promise."

~~152.~~249. Meta never corrected its representations from March 2021 to say that adults could still interact with minors on Instagram. On the contrary, it went to great lengths to make people believe that they could not.

~~153.~~250. Meta also never disclosed or warned the public of the full extent to which it was facilitating these incredible harms.

~~154.~~251. In 2022, Meta learned of even more sextortion related incidents occurring in connection with these known defects and lack of safety features. The following are just two,

a. On March 25, 2022, 17-year-old Jordan DeMay was the victim of Instagram. Like M.D., when Jordan headed up to his room for the night everything was fine – and all of that changed in a matter of hours, as the result of Instagram settings and business choices. *See DeMay et. al. v. Meta Platforms, Inc. et al.*, L.A. Sup. Ct., Case No. 24SMCV00732 (filed Jan. 31, 2024).

b. Less than two months later, on May 11, 2022, an Instagram predator sextorted 14- year-old John Doe. *See A.C. and John Doe v Meta Platforms, Inc.*, N.D. Cal., Case No. 4:23-cv-00646 (filed Feb. 13, 2023).

~~155.~~252. Same in early 2023, and the following is just one of those,

a. On April 25, 2023, 17-year-old Harry Burke was the victim of Instagram sextortion. Like Jordan and M.D., when Harry headed up to his room for the night everything was fine – and all of that changed in a matter of hours, as the result of Instagram settings and business choices. *See Carol Todd et. al. v. Meta Platforms, Inc. et al.*, L.A. Sup. Ct., Case No. 24SMCV04957 (filed Oct. 10, 2024).

~~156.~~253. Yet Meta stayed the course. It did not apply private-by-default settings to all teen accounts (including existing users) and several other safety features designed to reduce the incidence sextortion related harms until the end of 2024. This was after Meta learned about the deaths of ~~both~~ J.W., M.D., ~~and~~ L.M.

~~157.~~254. Even then, however, the changes Meta claims to have made at the end of 2024 appear to once again be misleading and/or defective. On December 6, 2025, for example,

the Wall Street Journal reported on workarounds whereby adults can connect with children and even exchange nude photos – despite Meta's promises to the contrary.[3]

~~158.~~255. While other testing suggests a loophole in the Android app that allows children to share their live location. Specifically, in one test, a child account reportedly was able to share their live location with an adult account that had been demanding nude images and sending threatening messages. While such functionality did not exist when one or ~~both~~ more users had an iPhone. Notably, Android phones are less expensive and, as such, this defect likely will have disproportionate impact on children from low income households and children using burner phones in order to access Instagram without parental knowledge and consent.

E. Meta Interferes with Its Users' Ability to Mitigate Harm

~~159.~~256. In addition to the above defects and failures to implement available and cost effective safety features, Meta's systems are set up on the back end in a manner that leaves vulnerable users powerless to protect themselves once the sextortion harms begin.

~~160.~~257. This includes broken reporting mechanisms, and Meta's refusal to act even on inpependant knowledge of harm to young users.

~~161.~~258. There are reported instances in the public record where Meta has failed to take down reported Child Sexual Abuse Material (CSAM) for several days, while harms were ongoing, where its reporting links and mechanisms did not work or led to dead ends, and where it ignored third party reporting of images associated with already identified and confirmed sextortion predators. *See, e.g.*, *A.C. and John Doe v Meta Platforms, Inc.*, N.D. Cal., Case No. 4:23-cv-00646 (filed Feb. 13, 2023) (involving 14-year-old victim subjected to sextortion harms on May 11, 2022).

[3] The Wall Street Journal, The Instagram Loophole That Can Enable Predators to Reach Teens, Dec. 6, 2025.

259. In fact, on information and belief, the images Plaintiff A.C. reported to Meta back in 2022 and then 2023 are among the most prolific images used by sextortion predators on the Instagram and Facebook apps to this day. They are images taken from a particular young woman, who posted them to Only Fans. In some instances, the images have identical metadata on the backend and, on information and belief, Meta has data that would easily link the images and/or predators utilizing such images fraudulently. Again, these images would have been reported and known to Meta repeatedly over the last few years; and yet, it is knowingly allowing such known abuses to continue without warning the public and/or the persons with whom these known predators are interacting in the virtual spaces Meta has constructed.

~~162.~~ But also, Meta's design defects work across its platforms. At one point, for example, Meta pushed to A.C. on his Facebook account a recommendation for a user that was using the same types of fake photos that had been used to sextort his son on Instagram. The same young woman from Only Fans, only this time, Meta pushed it to A.C.'s Facebook account.

~~163.~~260. The January 2024 Contagion Research Institute report confirms (attached as **Exhibit ~~B~~A**), including the fact that "Victims have repeatedly suggested that Instagram took no action on reports made against sextortion accounts."

~~164.~~261. This is troubling in any instance, and more so where the victims are children who trust and are relying on Meta to fulfill its promises.

~~165.~~262. Discovery will be required in this case to determine whether these children ~~M.D. or L.M.~~ reported the predators to whom Meta connected them, and whether law enforcement or other third parties put Meta on notice of these predators prior to when it made such connections.

~~166.~~263. Based on what Plaintiffs know at this time, however, it is possible if not

likely that Meta had actual knowledge that these predators were abusing children on its Instagram and Facebook platforms, and simply chose to do nothing. At the very least, Meta had a duty to warn ~~M.D. and L.M~~each and every one of these plaintiffs.

F. Young Users' Incomplete Brain Development Renders Them Particularly Susceptible to Manipulative Technologies with Diminished Capacity to Eschew Self-Destructive Behaviors and Less Resiliency to Overcome Negative Social Media Influences

~~167.~~264. The human brain is still developing during adolescence in ways consistent with adolescents' demonstrated psychosocial immaturity. Specifically, adolescents' brains are not yet fully developed in regions related to risk evaluation, emotional regulation, and impulse control.

~~168.~~265. The frontal lobes - and in particular the prefrontal cortex - of the brain play an essential part in higher-order cognitive functions, impulse control and executive decision-making. These regions of the brain are central to the process of planning and decision-making, including the evaluation of future consequences and the weighing of risk and reward. They are also essential to the ability to control emotions and inhibit impulses. MRI studies have shown that the prefrontal cortex is one of the last regions of the brain to mature.

~~169.~~266. During childhood and adolescence, the brain is maturing in at least two major ways. First, the brain undergoes myelination, the process through which the neural pathways connecting different parts of the brain become insulated with white fatty tissue called myelin. Second, during childhood and adolescence, the brain is undergoing "pruning" - the paring away of unused synapses, leading to more efficient neural connections. Through myelination and pruning, the brain's frontal lobes change to help the brain work faster and more efficiently, improving the "executive" functions of the frontal lobes, including impulse control and risk evaluation. This shift in the brain's composition continues throughout adolescence and continues into young adulthood.

~~170.~~267. In late adolescence, important aspects of brain maturation remain incomplete, particularly those involving the brain's executive functions and the coordinated

activity of regions involved in emotion and cognition. As such, the part of the brain that is critical for control of impulses and emotions and mature, considered decision-making is still developing during adolescence, consistent with the demonstrated behavioral and psychosocial immaturity of juveniles.

~~171.~~268. As acknowledged in now public Meta documents, Meta's social media products are designed to exploit minor users' diminished decision-making capacity, impulse control, emotional maturity, and psychological resiliency caused by users' incomplete brain development.

~~172.~~269. Meta knows that because its minor users' frontal lobes are not fully developed, such users are much more likely to sustain serious physical and psychological harm through their social media use than adult users.

~~173.~~270. Nevertheless, it has failed to design Instagram and Facebook with any protections to account for and ameliorate the psychosocial immaturity of its minor users.

~~174.~~271. On the contrary, Meta has designed its products to exploit these vulnerabilities at the expense of its users and for its own financial gains.

G. Instagram and Facebook are ~~is a~~ Products

272. Meta coded, engineered, manufactured, produced, assembled, and operates Facebook and Instagram, two of the world's most popular social media products, and placed the same into the stream of commerce. In 2022, two billion users worldwide were active on Instagram each month, and almost three billion were monthly active users of Facebook. This enormous reach has been accompanied by enormous damage for Plaintiffs and other adolescent users.

273. The Facebook and Instagram products were made and distributed with the intent to be used or consumed by the public as part of the regular business of Meta, the seller and/or distributor of Facebook and Instagram. Facebook and Instagram are not services; rather, they are

akin to tangible products for purposes of product liability law. When installed on a consumer's device, the Meta products have a definite appearance and location, and are operated by a series of physical swipes and gestures. Facebook and Instagram are personally moveable, and cannot be credibly construed as simply "ideas" or "information."

~~175. Instagram is an image-centric social media application where users can upload and share photos and videos. Meta earns advertising revenue through maximizing the amount of time users spend on Instagram and their level of engagement. The greater the amount of time that young users spend using the Instagram, the greater the advertising revenue Meta earns.~~

~~176.~~274. Meta designs, manufactures, and otherwise operates the Instagram and Facebook products in the same manner irrespective of the location where the product is being used.

~~177.~~275. Instagram and Facebook are ~~is a~~ social media products designed to be used by minors and actively marketed to minors globally. Meta is aware that large numbers of children under the age of 13 use its products despite user terms and Meta's "Terms of Use," which purport to restrict use to individuals who are 13 or older.

~~178.~~276. Despite this knowledge, Meta does not reasonably limit, safeguard or otherwise protect such children. On the contrary, it leans into this demographic.

~~179.~~277. Meta actively markets its social media products to minors – via a single, global strategy and global team – across the world, representing that Meta is designed for use by and safe for minors. Meta markets to minors globally through its own marketing efforts and design. But also, it works with and actively encourages advertisers to create ads targeted at and appealing to teens, and even to children under the age of 13.

~~180.~~278. The following are just some quotes from Meta internal documents concerning minors and Meta's social media products, supporting the above allegations:

a. "The Young Ones are the Best Ones"

b. Users who join Facebook as 13-year-olds "have an LTV [lifetime value] of approximately $350, higher than all other teen ages (13-18), due to their very high long-term retention."

c. "The difference in long term retention can be dramatic, with the people who signed up for Facebook when they were young teens being 100% higher."

d. "Teens strongly influenced preteens' understanding of what and how frequently to share on Instagram."

e. Instagram researcher: "teens are often the ones that other members of the household learn about not only Instagram, but social media in general through."

f. Armed with these insights, Meta concluded it should "acquire teens as young as possible."

g. "Teens: Let's always build and prioritize with them in mind."

h. Instagram CEO: "Mark [Zuckerberg] is suggesting that teen time spent be our top goal in 2017."

i. 2018: "Winning Teens = Winning Generations."

j. 2021: "Youth and Teens are critically important to Instagram.")

k. "capturing the teen user cohort on IG is critical."

l. "Acquiring new teen users is mission critical to the success of Instagram."

m. "Can we take this a step further and use school networks as a lever for acquisition?"

n. "How can we position Instagram as integral to navigating school relationships, especially during transition periods?"

o. "we will need to invest in virality within school communities to get teens and their friends on IG."

~~181.~~279. Meta also internally acknowledged that Instagram and its various features are products. The following are from just some Meta testimony and documents:

a. "[e]ngaging the vast majority of teens in an area / school with our products is crucial to driving overall time spent in the same area." (Emphasis added).

b. "We released a high volume (100+ in H1 2021) of product launches, 17 leading to integrity regressions." (Emphasis added).

c. Recommendation from a senior UX research leader at Instagram, which Meta did *not* follow: "Because our product exploits weaknesses in the human psychology to promote product engagement and time spent [and that because of our reliance on AI, we cannot currently control for when content is being strategically leveraged to manipulate the opinions and moods of individual people] if we are committed to the wellbeing of individuals, we need to a) alert people to the effect that the product has on their brain … and b) provide them with tools to have more control over their own experience." (Emphasis added).

d. "Product features that are designed to exploit insecurity, or provide a dopamine rush (likes, notification, the pull-down-to-see, the infinite scroll, etc), to increase time spent, are inherently at odds with well-being and take away from people's ability to consciously focus[] on activities that add value to their lives." (Emphasis added).

e. And, as it related to internal survey results in July 2021, showing that 13% of 13- to 15-years-old had received unwanted sexual advances on Instagram in the

past seven days, overwhelmingly from strangers, a Meta employee wrote, "they are experiencing these issues…facilitated by the product design of Instagram" (emphasis added).

H. Plaintiffs Expressly Disclaim Any and All Claims Seeking to Hold Meta Liable as the Publisher or Speaker of Any Content Provided, Posted, or Created by Third Parties

~~182.~~280. Plaintiffs' claims arise from Meta's status as designer, manufacturer, marketer, operator, and distributor of dangerously defective social media products that were used by children in the United Kingdom and United States, as Meta intended, as well as Meta's own statements and actions.

~~183.~~281. They are not based on Meta as the speaker or publisher of any third-party content.

~~184.~~282. Meta further failed to warn minor users and their parents of known dangers arising from anticipated use of its social media products, as set forth in detail herein.

~~185.~~283. Plaintiffs' claims seek to hold Meta accountable for its own allegedly wrongful acts and omissions, not for the speech of others or for any good faith attempt by Meta to restrict access to objectionable content.

~~186.~~284. Plaintiffs are not asking or even suggesting that Meta censor, review, or restrict any content whatsoever on its app. Instead, Meta has the ability and obligation to make its products safer for its minor users by making unilateral *product* changes and by providing reasonable and adequate warnings to consumers of known dangers and harms caused by use of its products.

~~187.~~285. The cost of such changes and warnings would have been nominal for Meta which at all relevant times had the technical ability to make all such changes.

~~188.~~286. Meta could manifestly fulfill its legal duty to design a reasonably safe social

media product and furnish adequate warnings of foreseeable sextortion hazards arising out of the use of anticipated use of Instagram without altering, deleting, or modifying the content of a single third-party post or communication.

VI. PLAINTIFFS' CLAIMS

COUNT I – PRODUCT LIABILITY (DESIGN DEFECT)

~~189.~~287. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~190.~~288. Meta's social media products are defective because the foreseeable risks of harm posed by the products' design could have been reduced or avoided by the adoption of reasonable alternative designs and the omission of the alternative designs renders the products not reasonably safe. This defective condition rendered the products unreasonably dangerous to persons or property and existed at the time the products left Meta's control, reached the user or consumer without substantial change in the condition and its defective condition was a cause of Plaintiffs' injuries.

~~191.~~289. Meta designed, manufactured, marketed, and sold social media products that were unreasonably dangerous because they were designed in a manner that effectively matched predators with children, shared the personal data of children with those predators, and exposed minor users to harms by design.

~~192.~~290. Meta's products were unreasonably dangerous because they contained numerous design characteristics that are not necessary for the utility provided to the user but are unreasonably dangerous and implemented by Meta solely to increase the profits derived from each additional user and the length of time Meta could keep each user dependent on their products.

~~193.~~291. At all times mentioned herein, Meta products failed to perform as safely as

an ordinary consumer and/or ordinary user would expect when used in an intended or reasonably foreseeable manner, and/or the risk of danger inherent in these products outweighed the benefits of said product.

~~194.~~292. As designed, Meta's products are not reasonably safe because they affirmatively direct minor users to predatory strangers, provide direct acces to minor users, incentivize such connections and make them appear safe, and because Meta deliberately failed to install and/or ensure effectiveness of safety features is claimed to have installed in its products.

~~195.~~293. It is feasible to design a product that protects minor users from these harms without altering, modifying, or deleting any third-party content posted on Meta's social media products. The cost of designing Meta's products to incorporate such safeguards would have been negligible, as Meta already knew, while the benefit would have been high in terms of reducing the quantum of mental and physical harm sustained by minor users and their families.

~~196.~~294. Defendants engage in other conduct designed to promote their harmful products as a means of increasing revenue. This includes but is not limited to efforts to encourage advertisers to design ads that appeal to minors; and product design features intended to attract and engage minors to these virtual spaces where these harms are then pushed in a manner intended to increase engagement, thereby increasing revenue to Meta at the cost of safety.

~~197.~~295. Reasonable consumers would not expect that Meta would knowingly expose them to such harms, much less in the manipulative and coercive manner it does.

~~198.~~296. Meta knew that these harms were being caused by their design designs and/or product defects and chose to do nothing. They essentially made the same choice made by Ford years ago in connection with the Pinto, which was to allow design based harms to consumers based on the calculation that allowing such harms was more profitable than addressing them.

~~199.~~297. As designed, Meta's product also is not reasonably safe because it does not enforce its explicit terms and promises regarding age and conduct.

~~200.~~298. Meta knows when a user is a minor. It has the information and means to ascertain with reasonable certainty each user's actual age and utilizes that knowledge for product development, marketing, and/or assessment, and ignores it when it comes to consumer safety.

~~201.~~299. Even if this were not the case, reasonably accurate age and identity verification is not only feasible but widely deployed by on-line retailers and internet service providers. The cost of incorporating age and identify verification into Meta's products would be negligible whereas the benefit of age and identity verification would be a substantial reduction in severe mental health harms, sexual exploitation, and abuse among minor users of Meta's products.

~~202.~~300. Meta's products also are defective for lack of parental controls, permission, and monitoring capability available on many other devices and applications.

~~203.~~301. Meta's advertising profit is directly tied to the amount of time that its users spend on Meta, while Meta designs its products to maximize the time users spend using the product by, among other things, increasing engagement through the exact types of invasive and inherently dangerous product features discussed herein.

~~204.~~302. It is feasible to make Meta' products exponentially safer for young users, including but not matchmaking for predators, utilizing privacy by default and other safety settings, and by providing working reporting mechanisms and acting on knowledge Meta has about such dangers and harms.

~~205.~~303. At all times relevant, Meta's products were not reasonably safe as designed because Meta did not include any safeguards it knew were necessary to prevent these specific harms.

~~206.~~304. It is reasonable for parents to expect that social media products that actively promote their platform to minors will undertake reasonable efforts to not matchmake children to predators by design, to not expose children through the unauthorized sharing of their personal information, and to act on independent knowledge of serious harms. It is feasible for Meta to design their products with reasonable safeguards, as evidenced by Meta's own internal records and findings.

~~207.~~305. It is reasonable for parents to expect that companies such as Meta, which actively promotes its products to minors and also actively claims that it cares about the safety of teen users, will undertake reasonable efforts to not matchmake teens with adult predators, not expose teens via unauthorized sharing of their personal data, and similar.

~~208.~~306. As a proximate result of these dangerous and defective design attributes of Meta's products decedents J.W., M.D., ~~and~~ L.M., E.H., and B.B. died.

~~209.~~307. Plaintiffs did not know, and in the exercise of reasonable diligence could not have known, of these defective designs in Instagram and Facebook and, as the result of Meta's concealment of the same, still do not understand and/or know about many of the defects at issue. But what they now know, including because of internal Meta documents that Meta has concealed for users, is enough.

~~210.~~308. As a result of the deaths of J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ caused by the improper conduct of Meta as set forth herein, Plaintiffs have been deprived of the expectation of pecuniary benefits which would have resulted from the continued life of J.W., M.D., L.M., E.H., and B.B.~~M.D. and L.M.~~, have lost contribution for support, companionship, society and household services, have incurred medical and funeral expenses, and have suffered and will continue to suffer severe mental anguish for the rest of their lives.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, any and all damages pursuant to 10 *Del. C.* § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT II – PRODUCT LIABILITY (FAILURE TO WARN)

~~211.~~309. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~212.~~310. Defendants' products are defective because of inadequate instructions or warnings because the foreseeable risks of harm posed by the products could have been reduced or avoided by the provision of reasonable instructions or warnings by the manufacturer and the omission of the instructions or warnings renders the products not reasonably safe.

~~213.~~311. This defective condition rendered the products unreasonably dangerous to persons or property, existed at the time the products left Meta's control, reached the user or consumer without substantial change in the condition in which it was sold and was a proximate cause of J.W., M.D., L.M., E.H., and B.B.~~M.D. and L.M.~~'s deaths.

~~214.~~312. Meta's products are unreasonably dangerous and defective because they contain no warning to users or parents regarding the dangerous design of Instagram and Facebook and lack of safeguards and/or defects in safeguards Meta claims to have employed.

~~215.~~313. Meta's products rely on highly complex and proprietary algorithms that are both undisclosed and unfathomable to ordinary consumers who do not expect that social media platforms and their features are designed to actively matchmake for predators and children.

~~216.~~314. The magnitude of harm these defects is known to Meta and includes sexual

exploitation and abuse, sextortion, and death.

~~217.~~315. The harms resulting from these defects has not only been documented over the last several years – before ~~both of~~ the deaths at issue in this Amended Complaint – in lawsuits and news reporting, but Defendants' only internal records confirm that Meta knew.

~~218.~~316. Meta knew and allowed these harms to continue anyway.

~~219.~~317. Defendants' products are unreasonably dangerous because they lack any warnings that foreseeable product use result in exposure, sexual exploitation, and sextortion or that Meta will push minor user's data to predatory adults or not act on reports and actual knowledge of such dangers.

~~220.~~318. It is feasible for Defendants to greatly reduce these harms. It is feasible as a matter of algorithmic programming, but also, it would have been simple as Meta putting teen users into working privacy settings, including settings that do not allow direct messaging from persons not already connected to them; it would have been as simple as not making Follower and Following data available to other users, as is done with many other platforms; it would even have been as simple as using age-related knowledge Meta actually has when protecting young users; it would have been as simple as providing young users with warnings when Meta had knowledge of risk factors, as it currently claims to do in instances where a teen receives a message from someone in a high risk location. There are many things that would have been simple for Meta to do, any one of which likely would have prevented the deaths at issue in this Amended Complaint. Yet, at all times relevant, Meta did none of them.

~~221.~~319. Meta knew about these harms, knew that users and parents would not be able to safely use Instagram without warnings, and failed to provide warnings that were adequate to make Instagram reasonably safe during ordinary and foreseeable use by children.

~~222.~~320. As a proximate result of Meta's failures to warn, J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ died.

~~223.~~321. Plaintiffs did not know, and in the exercise of reasonable diligence could not have known, of these defective designs in Instagram and Facebook and, as the result of Meta's well-documented efforts to conceal the same.

~~224.~~322. As a result of the deaths of J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ caused by Meta's failures to warn, Plaintiffs have been deprived of the expectation of pecuniary benefits which would have resulted from the continued life of J.W., M.D., L.M., E.H., and B.B.~~M.D. and L.M.~~, have lost contribution for support, companionship, society and household services, have incurred medical and funeral expenses, and have suffered and will continue to suffer severe mental anguish for the rest of their lives.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, any and all damages pursuant to 10 *Del. C.* § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT III - NEGLIGENCE

~~225.~~323. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~226.~~324. At all relevant times, Defendants had a duty to exercise reasonable care and caution for the safety of individuals using their products, such as J.W., M.D., L.M., E.H., and B.B.~~M.D. and L.M.~~

~~227.~~325. Meta owes a heightened duty of care to minor users of its products both

because of it is designing its products in a manner that affirmatively contributes to and/or causes such dangers and because adolescents' brains are not fully developed, which results in a diminished capacity to make good decisions regarding their social media usages, eschew self-destructive behaviors, and overcome emotional and psychological harm from negative and destructive social media encounters and much more susceptible to the types of dangers at issue in this Amended Complaint.

~~228.~~326. As a product manufacturer marketing and selling products to consumers across the world, including in the U.S. and Delaware, Meta owed a duty to exercise ordinary care in the manufacture, marketing, and sale of its products, including a duty to warn minor users and their parents of hazards that Meta knew to be present, but not obvious, to underage users.

~~229.~~327. As a business owner, Meta owes its users who use Meta's products and from whom Meta derives billions of dollars per year in advertising revenue a duty of ordinary care substantially similar to that owed by physical business owners to their business invitees.

~~230.~~328. Meta had a duty to refrain misrepresenting the safety of its products, and to not design those products in a manner it knew to be causing the harms identified herein to known minors who would not otherwise be exposed to such harms.

~~231.~~329. Meta benefited directly and substantially from its continued misconduct, knew it was causing harm, and knew it was benefiting in this manner.

~~232.~~330. Meta had a duty to evaluate and address the performance of its technologies and ensure that it was not exposing, encouraging, and directing vulnerable children to dangerous and deadly predators as a matter of product design.

~~233.~~331. Meta had a duty to employ and train personnel to appropriately and reasonably respond to notice and actual knowledge of these design-based harms.

~~234.~~332. Meta had a duty to design, develop, program, manufacture, distribute, sell, supply, and/or operate its products to ensure that it did not manipulate users and/or otherwise expose, encourage, and direct them to such harms.

~~235.~~333. Meta was negligent, grossly negligent, reckless and/or careless in that it failed to exercise ordinary care and caution for the safety of underage users, like J.W., M.D., L.M., E.H., and B.B~~M.D. and L.M~~.

~~236.~~334. Meta was negligent in failing to conduct adequate testing, but also, in having conducted testing and then ignored the evidene and conclusions that Meta was causing these exact harms as a matter of design. Meta has extensive internal research and/or documents and communications evidencing that it knew it was causing these exact harms by design, and failed to take reasonable steps to prevent such design-based harms.

~~237.~~335. Meta was negligent in failing to provide adequate warnings about the dangers associated with the use of its products and in failing to advise users and their parents about how and when to safely use its application and features.

~~238.~~336. Meta was negligent in failing to fully assess, investigate, and restrict the use of specific Meta settings and tools by adults to sexually solicit, abuse, manipulate, and exploit minor users of its products.

~~239.~~337. Meta was negligent in failing to provide users and parents the tools to ensure that its products are used in a limited and safe manner by minor users.

~~240.~~338. Meta knew that children were dying after being sextorted by adult predators because of Meta's tools and design designs. Internal Meta documents admit to actual knowledge of these harms and the failure of Meta leadership to act to reduce them in a reasonable and timely manner.

~~241.~~339. As a proximate result of Meta' negligence, dozens of children have died. ~~Two~~ Just five of those children – J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ are at issue in this amended complaint.

~~242.~~340. Plaintiffs did not know, and in the exercise of reasonable diligence could not have known, of Meta's negligence and breach of duties because Meta concealed the same.

~~243.~~341. As a result of the deaths of J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ caused by Defendants' negligence, Plaintiffs have been deprived of the expectation of pecuniary benefits which would have resulted from the continued life of J.W., M.D., L.M., E.H., and B.B.~~M.D. and L.M.~~, have lost contribution for support, companionship, society and household services, have incurred medical and funeral expenses, and have suffered and will continue to suffer severe mental anguish for the rest of their lives.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, any and all damages pursuant to 10 Del. C. § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT IV - FRAUDULENT CONCEALMENT AND/OR MISREPRESENTATION

~~244.~~342. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~245.~~343. As set forth in more detail above, Defendants knew about the defective condition of Instagram and Facebook and that Instagram and Facebook posed serious risks to users like and including J.W., M.D., L.M., E.H., and B.B~~M.D. and L.M~~.

~~246.~~344. Meta was under a duty to tell the public the truth and to disclose the

defective condition of their products and that their products posed serious health risks to users, particularly youth.

~~247.~~345. Defendants breached their duty to the public, users, and their parents, including Plaintiffs, by actively concealing, failing to disclose, and making misstatements about the serious safety risks presented by Meta as well as the effectiveness of Meta's claimed safety features.

~~248.~~346. Meta was explicitly told by employees that it was not doing enough, that consumers and regulators expected and understood that it was doing more, and that even the safety features Meta claimed to have installed were defective.

~~249.~~347. Meta knew of these risk and shortcomings based on its own records, its own studies, design-related decisions, and information conveyed to it by third parties; and with this knowledge, it intentionally concealed these findings in order to not lose users and advertising revenue, and to induce youth, including J.W., M.D., L.M., E.H., and B.B~~M.D. and L.M.~~, to continue using Instagram and Facebook and parents, including Ros, Mark, ~~and~~ Tricia, Tamia, Tim, Shannon, Brittney, and Parker to trust in Meta's safety representations and to allow their children – children who showed little to ~~not~~ interest in other social media products – to use Instagram and/or Facebook specifically.

~~250.~~348. Meta made numerous material representations downplaying any potential harm associated with Instagram and Facebook and reassuring the public, Congress, and parents, including Plaintiffs, that its platform and related product features were safe, including but not limited to,

a. Dozens of public statements published in both the United States and the United Kingdom regarding Meta's commitment to safety, including and especially as it relates to teen users.

b. This includes a Facebook Post by Meta CEO Mark Zuckerberg on October 5, 2021, denying allegations made by a Meta whistleblower and specifically representing that Meta was doing everything possible to keep kids safe:

> I'm particularly focused on the questions raised about our work with kids. I've spent a lot of time reflecting on the kinds of experiences I want my kids and others to have online, and it's very important to me that everything we build is safe and good for kids.
>
> The reality is that young people use technology. Think about how many school-age kids have phones. Rather than ignoring this, technology companies should build experiences that meet their needs while also keeping them safe. We're deeply committed to doing industry-leading work in this area.

c. Meta CEO Mark Zuckerberg made similar and numerous representations in sworn testimony before Congress, but also, and importantly, Meta continued to provide countless safety related assurances in its global marketing campaign – commercials and advertising on television, as well as strategic partnership that infiltrated schools.

d. Meta paid the National PTA and Scholastic to conduct an extensive outreach campaign targeting schools and families. As a teacher, Tricia was aware of these representations and understood that Instagram and Facebook were~~was~~ safe for kids based on Meta's explicit representations that they were~~it was~~.

e. In Meta's own words, it chose to partner with these organizatinos because they were "trusted, respected organizations" with "significant credibility" that could "be a public validator" for the company and "get our materials into the hands of parents, grandparents, and educators at scale." Meta's agreements with

these organizations "include significant website placement, social media promotion, targeted physical distribution, community activations, and post-campaign surveys."

~~251.~~349. Meta knew that children were suffering sexual exploitation and sextortion as a result of their design decisions years before J.W., M.D., L.M., E.H., and B.B. ~~M.D. or L.M.~~ died.

~~252.~~350. Instead of warning consumers about these very real dangers, Meta made the business decision to downplay the dangers and convince consumers, instead, that no such danger existed.

~~253.~~351. For example, in 2021, Meta announced to the world that it would be would be "restricting DMs between teens and adults they don't follow." But this was not what Meta did.

~~254.~~352. While "private by default was originally supposed to be for all users," Meta instead launched a feature it applied only to "new users under the age of 16"—not existing teen users, new 17- or 18-year old users, or new teen users who lied about their birthday.

~~255.~~353. Based on J.W., M.D., L.M., E.H., and B.B.'s ages, their ~~M.D.'s age, his~~ parents would have understood this safety feature as applying to ~~him~~each of them. In the case of those already using Meta's products at the time,~~Since he was already an Instagram user at the time, however,~~ Meta did not apply it to ~~him~~them. While this safety feature should have applied to L.M. and B.B. since ~~he~~ they were under 16 ~~was only 13~~ at the time ~~he~~ they began using ~~Instagram~~ Meta's products in 2023; but on information and belief, it did not work.

~~256.~~354. It shoud not come as a surprise to Meta that it did not work, since Meta's own testing post-launch determined that it was not working. An internal Meta service showed that 13% of 13- to 15-years-old had received unwanted sexual advances on Instagram in the past seven

days, overwhelmingly from strangers. Meta employees acknowledged, "they are experiencing these issues…facilitated by the product design of Instagram" and even though Meta purported to have fixed this defect. In February 2022, a "sitewide emergency event" revealed that teens were *still* "receiving DM requests from unconnected adults, breaking [the] public commitment that we made." This was more than a year before ~~either M.D. or L.M.~~these children died, and yet, Meta never told ~~either set of~~and of their parents the truth. It kept the truth a secret to save its own bottom line.

~~257.~~355. "[U]nwanted DM requests" remained a serious risk issue for teens long after Meta's "private by default" announcement, with Meta conceding (internally, never externally) that "there have been many gaps in fulfilling our promise."

~~258.~~356. Meta did not do what it promised Plaintiffs in 2021 that it had done. In fact, it did not even approach those promises until the end of 2024, though Plaintiffs cannot even be certain that it did what it said in late 2024 given Meta's history of fraud and broken promises. But regardless of whether Meta fixed these systemic failures in late 2024, it knew about them and did not fix them any of the years prior. If Meta had done what it promised in 2021, 2022, or even as late as 2023, ~~M.D. and L.M.~~these children would not have died the way they did – Meta would not have connected them to these predators by design or provided these predators with the critical tools needed to directly connected and then be able to threaten these children with immediate exposure to the entirety of their friend and family network.

~~259.~~357. Meta's many representations regarding the safety of its produces were false, and Meta knew that its representations were false when the statements were made.

~~260.~~358. Meta intentionally failed to disclose the serious safety risks it knew about to the public, users, and their parents, including Plaintiffs. Such risks were known only to Meta

through its internal testing, reports, and recommendations, and other information known to Meta, and the public, users, parents, and even regulators could not have discovered such serious risks and fraud.

~~261.~~359. The public, users, and their parents, including Plaintiffs, did not know of the serious safety risks posed by the design of Instagram. But Meta knew~~.~~.

~~262.~~360. By intentionally concealing and failing to disclose defects inherent in the design of Instagram, Meta knowingly and recklessly misled the public, users, and their parents, including Plaintiffs, into believing these products were safe for children to use.

~~263.~~361. By intentionally making numerous material representations, downplaying any potential harm associated with Instagram and Facebook and teen users, and reassuring the public, lawmakers, and parents, including Plaintiffs, that it was safe, Meta fraudulently or, in the alternative, negligently misled the public, users, and parents, including Plaintiffs, into believing that Instagram and Facebook were ~~was~~ safe for children to use.

~~264.~~362. Meta intended for public, users, and their parents, including Plaintiffs, to rely on its representations about the safety of Instagram and Facebook.

~~265.~~363. Meta knew that its concealment, misstatements, and omissions were material. A reasonable person, including Plaintiffs, would find information that impacted the users' health, safety, and well-being, such as serious adverse health risks associated with the use of Instagram and Facebook and dangerous practices Meta engaged in with children's privacy and personal data, to be important when deciding whether to use, or continue to use, those products.

~~266.~~364. The public, users, and their parents, including Plaintiffs, reasonably relied on the representations made by Meta about the safety of Instagram and Facebook for use by children.

~~267.~~365. Meta intended to deceive the public, users, and their parents, including Plaintiffs, by concealing the defects in the design of Instagram and Facebook which made the products unsafe.

~~268.~~366. As a direct and proximate result of Meta's material omissions, misrepresentations, and concealment of material information, Plaintiffs were not aware and could not have been aware of the facts that Meta concealed or misstated, and therefore justifiably and reasonably believed that Instagram and Facebook were ~~was~~ safe for children to use.

~~269.~~367. If the serious safety risks presented by the design of Meta had been disclosed, the public, users, and their parents, including Plaintiffs, reasonably would have acted differently and/or would have ceased use of Instagram and/or Facebook.

~~270.~~368. Meta's concealment and Plaintiffs' reliance on Meta's representations about the safety of Instagram and Facebook were substantial factors in causing harm to Plaintiffs.

~~271.~~369. Meta's conduct, as described above, was intentional, fraudulent, willful, wanton, reckless, malicious, fraudulent, oppressive, extreme, and outrageous, and displayed an entire want of care and a conscious and depraved indifference to the consequences of its conduct, including to the health, safety, and welfare of its customers, and warrants an award of punitive damages in an amount sufficient to punish Meta and deter others from like conduct.

~~272.~~370. As a proximate result of Meta's fraud ~~M.D.~~J.W., M.D., L.M., E.H., and B.B. ~~and L.M.~~ died. Plaintiffs did not know, and in the exercise of reasonable diligence could not have known, of Meta's fraud.

~~273.~~371. As a result of the deaths of J.W., M.D., L.M., E.H., and B.B~~M.D. and L.M.~~ caused by Defendants' negligence, Plaintiffs have been deprived of the expectation of pecuniary benefits which would have resulted from the continued life of J.W., M.D., L.M., E.H., and

B.B.~~M.D. and L.M.~~, have lost contribution for support, companionship, society and household services, have incurred medical and funeral expenses, and have suffered and will continue to suffer severe mental anguish for the rest of their lives.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, any and all damages pursuant to 10 *Del. C.* § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT V - INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

~~274.~~372. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~275.~~373. As the preceding allegations demonstrate, Defendants' conduct was intentional, reckless, extreme and outrageous in failing to implement adequate safety features or provide warnings to consumers in connection with the use of Instagram and Facebook, despite Defendants' having actual knowledge of the harms of the propensity of Defendants' technologies and/or programming decisions specifically targeting minor users.

~~276.~~374. In light of children's developmental vulnerabilities and the premium value assigned to their usage of Meta's platform~~s~~d – that is, Defendants expressly recognize that minor users are the most significant and/or profitable in terms of their long-term success – Meta's conduct in targeting children like and including the ones at issue in this amended complaint was outrageous.

~~277.~~375. Meta's conduct caused severe emotional distress to Plaintiffs, all of whom lost their children to harms occurring as the result of Meta's deliberate and exploitative misconduct.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, any and all damages pursuant to 10 Del. C. § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT VI –NEGLIGENCE *PER SE* AND VIOLATION OF STATUTE

~~278.~~376. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~279.~~377. Defendants' conduct as set forth herein constitutes a violation of 6 *Del. C.* §1201C *et seq* ("Online and Personal Privacy Protection").

~~280.~~378. Defendants' conduct constitutes negligence *per se.*

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, any and all damages pursuant to 10 Del. C. § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT VII – UNJUST ENRICHMENT

~~281.~~379. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~282.~~380. As a result of Defendants' conduct detailed herein, Defendants received a benefit. Because Defendants' advertising profits are directly tied to the number of user accounts and the amount of time those users spend Instagram and Facebook, Defendants benefited directly from J.W., M.D., L.M., E.H., and B.B.~~M.D. and L.M.~~'s use of their products and product features,

and it would be unjust to allow them to retain such benefits.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, any and all damages pursuant to 10 Del. C. § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT VIII – INVASION OF PRIVACY

~~283.~~381. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~284.~~382. Defendants intentionally intruded upon Plaintiffs' solitude, seclusion, or private affairs by knowingly designing their products with features that were intended to, and did,

a. Minimize user control over what information each of the minor Plaintiffs' received while using Instagram and Facebook, in a manner that was both harmful, but also, designed to deprive them of access and/or choice.

b. Covertly manipulate and exploit user autonomy in multiple ways while each of the minor Plaintiffs used Instagram and Facebook.

c. Greatly exceed the limits of consent provided by each Plaintiff and/or Plaintiff parent, if any, with regard to Defendants collection and use of J.W., M.D., L.M., E.H., and B.B.'s ~~M.D. and L.M.'s~~ data, use of Defendants' products by J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~, and receipt of communications from Meta by their minor children and/or in their homes.

~~285.~~383. These intrusions are highly offensive to a reasonable person, particularly given Meta's interference with the fundamental right of parenting and its exploitation of children's

special vulnerabilities for commercial gain.

~~286.~~384. Plaintiffs were harmed by Meta's invasion of privacy, as detailed herein.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, any and all damages pursuant to 10 Del. C. § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT IX – WRONGFUL DEATH

~~287.~~385. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~288.~~386. Plaintiffs are the Administrators and Personal Representatives of the Estates of J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~

~~289.~~387. As the direct and proximate result of the conduct of Defendants and the defective nature of their products, as set forth above, decedents J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ suffered wrongful death.

~~290.~~388. Plaintiffs seek damages, including loss of financial support, loss of society, funeral expenses, estate administration expenses, and noneconomic damages including pain and suffering, anxiety and anguish, and, as permitted, and where applicable, punitive damages.

WHEREFORE, plaintiffs demand judgment against defendants, jointly and severally, for special and general damages, including pain and suffering, punitive damages, damages for wrongful death, pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, the costs

of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

COUNT X - SURVIVAL

~~291.~~389. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs as if they were set forth in full.

~~292.~~390. Plaintiffs have been appointed as Administrators of the Estates of J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~

~~293.~~391. As a consequence of their injuries, decedents J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ experienced conscious pain and suffering.

~~294.~~392. A claim against defendants for damages sufficient to compensate decedents J.W., M.D., L.M., E.H., and B.B. ~~M.D. and L.M.~~ for their pain and suffering and medical expenses has survived to plaintiffs as Administrators of the Estates of J.W., M.D., L.M., E.H., and B.B.~~M.D. and L.M.~~, pursuant to 10 *Del. C.* §3701.

WHEREFORE, plaintiffs demand judgment against defendants for their special and general damages, including pain, suffering and mental anguish, punitive damages, any and all damages for wrongful death pursuant to 10 *Del. C.* § 3721 *et seq*, Delaware's Wrongful Death Act, any and all damages pursuant to 10 Del. C. § 3701, the costs of this action, plus pre-judgment and post-judgment interest and other such relief as the Court finds just.

RHOADES & MORROW LLC

/s/ Joseph J. Rhoades
Joseph J. Rhoades, Esquire (I.D. 2064)
Stephen T. Morrow, Esquire (I.D. 4891)
1225 King Street, 12th Floor
Wilmington, Delaware 19801
joe.rhoades@rhoadeslegal.com

stephen.morrow@rhoadeslegal.com
302-427-9500

SOCIAL MEDIA VICTIMS LAW CENTER PLLC
Matthew P. Bergman (Pro Hac Vice anticipated)
matt@socialmediavictims.org
Laura Marquez-Garrett (Pro Hac Vice anticipated)
Laura@socialmediavictims.org
600 1st Avenue, Suite 102-PMB 2383
Seattle, WA 98104
206-741-4862

DATE: February 27, 2026~~February 27, 2026~~~~February 22, 2026~~ Attorneys for Plaintiffs

EXHIBIT A

LAURA MARQUEZ-GARRETT (SBN 221542)
laura@socialmediavictims.org
SOCIAL MEDIA VICTIMS LAW CENTER
821 Second Avenue, Suite 2100
Seattle, WA 98104
Telephone: (206) 741-4862
Facsimile: (206) 957-9549

KEVIN M. LOEW (SBN 238080)
kloew@waterskraus.com
WATERS, KRAUS & PAUL
222 North Pacific Coast Hwy, Suite 1900
El Segundo, California 90245
Telephone: (310) 414-8146
Facsimile: (310) 414-8156

Attorneys for Plaintiffs

IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

A.C. and **JOHN DOE**,

Plaintiffs,

vs.

META PLATFORMS, INC., *formerly known as* FACEBOOK, INC.; **SNAP, INC**.; and **DOES 1 – 100, INCLUSIVE**,

Defendants.

Case No.: 22STCV36188

COMPLAINT FOR

(1) STRICT PRODUCT LIABILITY (DESIGN DEFECT)
(2) STRICT PRODUCT LIABILITY (FAILURE TO WARN)
(3) NEGLIGENCE
(4) VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, CAL. BUS & PROF. CODE §§ 17200, ET SEQ.
(5) UNJUST ENRICHMENT
(6) INVASION OF PRIVACY
(7) INFLICTION OF EMOTIONAL DISTRESS

JURY TRIAL DEMAND

COME NOW PLAINTIFFS A.C. and JOHN DOE and allege as follows:

"In these digital public spaces, which are privately owned and tend to be run for profit, there can be tension between what's best for the technology company and what's best for the individual user or for society. Business models are often built

> around maximizing user engagement as opposed to safeguarding users' health and ensuring that users engage with one another in safe and healthy ways. . . . Technology companies must step up and take responsibility for creating a safe digital environment for children and youth. Today, most companies are not transparent about the impact of their products, which prevents parents and young people from making informed decisions and researchers from identifying problems and solutions."

Protecting Youth Mental Health, The U.S. Surgeon General's Advisory (December 7, 2021)

Plaintiff A.C., individually and on behalf of his minor child, John Doe, brings this action for personal injuries against Meta Platforms, Inc., formerly known as Facebook, Inc., and Snap, Inc., for injuries caused to each of them as a result of John Doe's use of the defective and inherently dangerous Instagram and Snapchat social media products and alleges as follows:

I. INTRODUCTION

1. This product liability action seeks to hold Defendants' Instagram and Snapchat products responsible for causing and contributing to the burgeoning mental health crisis perpetrated upon the children and teenagers of the United States by Meta and Snap, and specifically for the injuries they caused Plaintiff A.C. and John Doe in 2022, when John Doe was only 14. John Doe and A.C.'s injuries were proximately caused by Defendants' defective and unreasonably dangerous Instagram and Snapchat products, including specific product features that are unnecessary to the functionality of their products and are known by them to be harmful to a significant number of their minor users. The injuries at issue in this lawsuit include but are not limited to anxiety, depression, exploitation, and related mental health harms suffered by John Doe and his father as a result of Defendant Meta and Snap's actions and failures to act.

2. Meta and Snap target and market their products to children and teens, representing to the public, and even Congress, that their social media products are not addictive and are designed to be fun and safe for kids, and that they use all available technologies to keep underage users safe.

3. In truth, however, Defendants' products are designed in a manner that encourages and assists minor users in evading parental authority and control, resulting in Defendants' distribution and profits from distribution of their products to millions of unauthorized, minor users;

Defendants have invested billions of dollars to design and develop addictive product features, including features designed to exploit minor users' physiological and psychosocial vulnerabilities; and Defendants have designed, and implement in the case of minor accounts, specific product features that promote and enable the connection of minors with predatory adults and resulting exploitation and abuse of the kinds at issue in this case. Moreover, Defendants then designed their products and processes in a manner that prevents parents from protecting their children from the harms being caused by and/or perpetrated because of Defendants' social media products.

4. Defendants know or should know of each of these product defects and/or inherently harmful product features, and the harms directly and proximately caused by them.

5. Meta and Snap do not warn users or parents about these known defects and/or inherently dangerous product features and, again, do not provide reasonable, accessible, and effectual reporting mechanisms for parents to protect their children from these harms. On the contrary, Defendants' reporting systems are designed and/or operated in such a defective manner that even parents who work in the technology industry are powerless to protect their children and others from identified harms.

6. Plaintiffs bring claims of strict liability based upon Defendants' defective design of their social media products that renders such products not reasonably safe for ordinary consumers or minor users. It is technologically feasible to design social media products that substantially decrease both the incidence and magnitude of harm to minors arising from their foreseeable use of Defendants' products with a negligible increase in production cost.

7. Plaintiffs also bring claims for strict liability based on Defendants' failure to provide adequate warnings to minor users and their parents of the danger of mental, physical, and emotional harms arising from foreseeable use of their social media products. The addictive qualities of Defendants' products and harms caused by their recommendation technologies, account settings, and other product features were known to Defendants but are unknown to minor users and their parents.

//

8. Plaintiffs also bring claims for common law negligence arising from Defendants' unreasonably dangerous social media products and their failure to warn of such dangers. Defendants knew, or in the exercise of ordinary care should have known, that their social media products were harmful to a significant percentage of their minor users and failed to redesign their products to ameliorate these harms or warn minor users and their parents of dangers arising out of the foreseeable use of their product.

9. Plaintiffs bring claims under California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code, §§17200, *et seq*. The conduct and omissions alleged herein constitute unlawful, unfair, and/or fraudulent business practices prohibited by the UCL.

10. Plaintiffs bring claims for invasion of privacy. Defendants' conduct detailed herein frustrated and intruded upon Plaintiff A.C.'s fundamental right to protect his child and to monitor and control his child's use of social media, and this intrusion occurred in a manner that was highly offensive to a reasonable person.

11. Lastly, Plaintiffs bring claims for intentional and/or negligent infliction of emotional distress against Defendant Meta. Meta is distributing a defective product and/or a product that is inherently harmful to a significant number of its minor users, and then deprives parents of any reasonable or effective means to report and put a stop to such harms. Even when Meta receives reports, it routinely does not act or acts in a manner insufficient to protect minor users from the reported harms, which failures foreseeably and proximately cause extreme stress, anxiety, and emotional harm to reporting parents, in this case, Plaintiff A.C.

II. PARTIES

12. Plaintiff A.C. is the parent and legal guardian of John Doe and John Doe is currently 15 years old, and both are residents of the state of Arizona. Plaintiff A.C. has not entered into a User Agreement or other contractual relationship with any of the Defendants herein in connection with John Doe's use of Defendants' products and disaffirms all agreements that John Doe may have entered with Defendants. As such, Plaintiff A.C. is not bound by any arbitration, forum selection, choice of law, or class action waiver set forth in any such agreements.

13. Defendant Meta Platforms, Inc., formerly known as Facebook, Inc., is a Delaware corporation with its principal place of business in Menlo Park, CA. Defendant Meta Platforms owns and operates the Facebook and Instagram social media platforms, which are made widely available to users throughout the United States, and manufactures and sells the Oculus virtual reality headset, which it operates directly via its Facebook social media platform, also made widely available to users throughout the United States.

14. At all times relevant hereto, Defendant Meta Platforms, Inc. was acting by and through its employees, servants, agents, workmen, and/or staff, all of whom were acting within the course and scope of their employment, for and on behalf of Meta Platforms, Inc.

15. Defendant Snap, Inc. is a Delaware corporation with its principal place of business in Santa Monica, CA. Defendant Snap owns and operates the Snapchat social media platform, an application that is widely marketed by Snap and available to users throughout the United States.

16. At all times relevant hereto, Defendant Snap Inc. was acting by and through its employees, servants, agents, workmen, and/or staff, all of whom were acting within the course and scope of their employment, for and on behalf of Snap Inc.

III. JURISDICTION AND VENUE

17. This Court has personal jurisdiction over Defendants because these defendants all have their principal places of business in California and are "at home" in this State.

18. Venue is proper in Los Angeles County because Snap is headquartered here.

IV. FACTUAL ALLEGATIONS

19. In late 2021, a Facebook whistleblower disclosed thousands of internal Meta documents to the United States Securities Exchange Commission (the "SEC") and Congress. The Facebook Papers prove known dangerous designs and design defects as well as operational decisions and calculations, and a causal relationship between use of Defendants' various social media products in their current form and resulting addiction, anxiety, depression, eating disorders, exploitation and grooming, and what Meta internally refers to as "SSI" (Suicide and Self Injury). While the Facebook Papers originate from Meta, they prove known dangerous designs and design

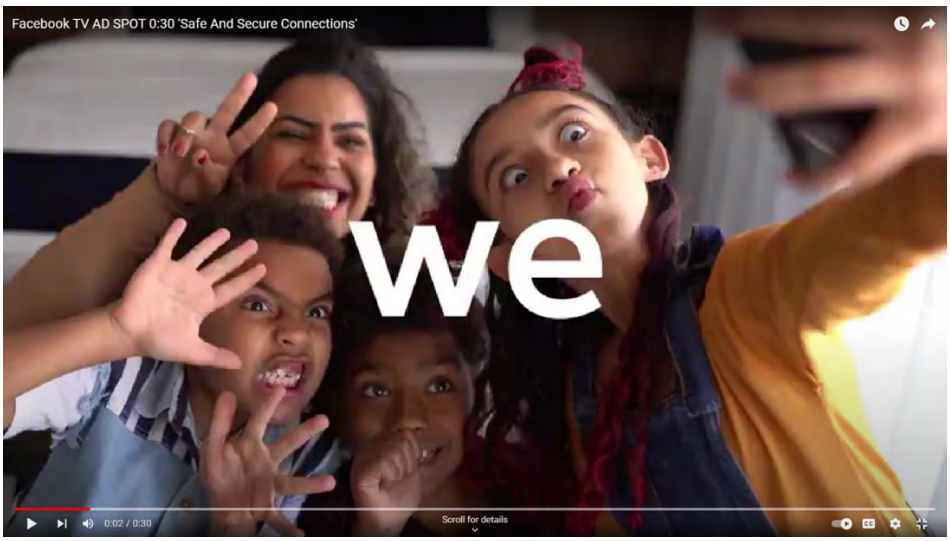
defects as well as other dangers caused by the social media products of both Defendants.[1]

20. Defendants have knowledge about the harms their products cause users, particularly teens, children, and other vulnerable user populations, and Defendants continue to operate their products in a harmful and dangerous manner anyway.

21. Defendants are making calculated cost-benefit business decisions and are prioritizing their already astronomical profits over human life.

A. Meta and its Facebook and Instagram Products

22. "Facebook connects people. It's what we do. And real connection can only happen on safe and secure platforms. That's why we build technology that gives you more control and helps keep you safe." These words are the opening lines from a television advertisement Meta—the creator of popular social media platform Facebook—launched earlier this year. As these words are spoken by a voice actor, images of smiling Facebook users—many of whom, like in the screenshot from this advertisement below, appear to be children—flash on screen. The advertisement goes on to identify a number of specific safety features, including "industry leading AI" that represent "tools that can protect—so you can connect."



[1] Examples of the Facebook papers have been published by the Wall Street Journal (https://digitalwellbeing.org/the-facebook-files-on-instagram-harms-all-leaked-slides-on-a-single-page/), Gizmodo (https://gizmodo.com/facebook-papers-how-to-read-1848702919), and other publishers, and have been disclosed to the SEC, Congress, and others on a global scale. Plaintiff expressly incorporate all such documents into this Complaint by reference, which are central and material to certain of Plaintiff's claims.

23. This is not a new message for Meta. Since the company's initial public offering (and before), Meta claimed that Facebook (and later, Meta's Instagram product) "include[s] robust safety tools" and "take[s] into account the unique needs of teenagers who use our service." It has repeated variations of these claims a staggering number of times in a wide variety of mediums. Over and over again, Meta has claimed that Facebook and Instagram are safe for children and teenagers to use because of the company's algorithmic and non-algorithmic safety tools.

24. Meta was founded in 2004 and is the world's largest social media company. While Instagram began as a simple photo-sharing application, which Meta purchased in 2012.

25. When Meta began, access to its products was limited to college students, with email and/or domain verification to confirm the same. Then, in September 2006, Meta opened Facebook up to everyone. It claimed that it provided access only to persons 13 and older, and that users under 18 should obtain parental consent. But it stopped verifying age or identity, to the point where Meta does not even verify existence of a valid email address – meaning that underage users and predators enter nonsense email addresses and Meta provides access to limitless Facebook and Instagram accounts anyway. These product changes have proven good for Meta's bottom line but resulted in the complete absence of any safety features for children and teens.

26. In 2009, Meta launched the "like" button product and, in 2011, it launched Facebook Messenger. By 2012, when Meta acquired the Instagram social media product, it was making rapid and significant changes to all its social media products – including Facebook and Instagram – which changes focused entirely on increasing engagement at any cost. This included product changes, as well as changes in data collection and advertising policies and procedures; essentially any change Meta could devise that might bolster engagement and revenue, particularly among children and teens, and create greater addiction and network effects features to ensure that those users would be locked-in to its social media products for years to come – but at the expense of user safety and autonomy.

27. To name only one example, Meta developed and patented its News Feed product, *see* U.S. Patent No. 8,171,128, "Communicating a newsfeed of media content on a member's

interactions in a social network environment" (filed August 11, 2006, granted May 1, 2012). The patent "describes keeping a profile of each person on the social network in a database, identifying relationships between said users, generating 'stories' based on the connections, and then creating a News Feed for each user."[2] Internal Meta documents confirm that in or around 2016 Meta made changes to operation of its News Feed product, which significantly increased engagement, at the expense of user safety. This was only one such change made by Meta in that time frame.

28. With the knowledge that teen and child users were Meta's only opportunity for growth in the United States, Meta ramped up its marketing to children and teens – including and specifically to children under the age of 13. It designed several new products and re-designed several existing products on its Facebook and Instagram platforms, launched and marketed games and emojis, and became significantly more involved with content creation. It also made it easier for kids to hide accounts and switch between accounts on a single device and, at one point, launched a campaign to ensure that all teens knew of their ability to open multiple accounts.

29. Meta also creates images and GIFs for users to post on their videos and pictures in connection with its Facebook and Instagram products. Meta has also acquired publishing rights to thousands of hours of music, which it provides to its users to attach to the videos and pictures that they post on Facebook and/or Instagram. The GIFs, images, and music are integral to the user's post and are, in fact, designed to encourage posting. Indeed, in many cases, the only content in a user's post is the image, GIF or music supplied by Meta. When users incorporate images, GIFs, and music supplied by Meta into their postings, Meta is functioning as a co-publisher of such content. A Facebook and/or Instagram user who incorporates images, GIFs or music supplied by Meta into their post is functionally equivalent to a novelist who incorporates illustrations into their story. Instagram can no longer characterize the images, GIFs, and music it supplies to its users as

[2] *See* https://www.zdnet.com/article/facebook-patents-the-news-feed/; *see also, e.g.* https://info.ipvisioninc.com/blog/4-creepy-facebook-patents-that-are-actually-real (discusses various, invasive social media products for which Meta has obtained patents, which Meta may or may not be using on its users – which information is known only to Meta); https://www.forbes.com/sites/nicolemartin1/2018/11/20/facebook-files-algorithm-patent-to-predict-who-you-live-with/?sh=3b987fe73544 (discussing Facebook patent application to use algorithms to determine who lives in the same household);

third-party content, just as the novelist cannot disclaim responsibility for illustrations contained in their book. Meta has made the deliberate decision to collaborate with its users in this regard and, as evidenced by Meta's internal documents, Meta's decision is motivated by the fact that such collaboration results in increased engagement, advertising revenue, and other profits for Meta itself.

30. Meta also has ownership and/or licensing, and other legal, rights in all third-party content, such that it is not "third-party content" at all. To name only one example, in 2012, Meta revised its Instagram Terms of Service to the following,[3]

> To help us deliver interesting paid or sponsored content or promotions, you agree that a business or other entity may pay us to display your username, likeness, photos (along with any associated metadata), and/or actions you take, in connection with paid or sponsored content or promotions, without any compensation to you.

Its current terms (effective January 4, 2022) are different, but still grant Meta the right to use all third-party content at Meta's sole and unilateral discretion and in connection with all its social media products.

31. Meta knows that it is harming teens yet, when faced with recommendations that would reduce such harms, Meta's leadership has consistently opted for prioritization of profit over the health and well-being of its teen users – including product changes that, if adopted by Meta, would have prevented harms at issue in this lawsuit.

B. Snap and its Snapchat Product

32. Snapchat was founded in 2011, by three Stanford college students, and was originally called *Pictaboo*. It started as a simple app with the idea that it would be nice to be able to send photos to friends that would disappear. Months after its launch, *Pictaboo* had only amassed 127 users,[4] however, so it changed its name to Snapchat and began marketing to and targeting high school students. Within a year, and with its new target audience of children and teens, Snapchat grew to more than 100,000 users.

[3] https://www.theverge.com/2012/12/18/3780158/instagrams-new-terms-of-service-what-they-really-mean
[4] *See* https://frozenfire.com/history-of-snapchat/

33. The Snapchat social media product quickly evolved from there, as its leadership made design changes and rapidly developed new product features intended to, and that did, increase its popularity among minors. This included video capabilities (2012); "Stories" and "Chat" features (2013); live video chat capabilities, text conversations, "Our Story," Geofilters, and Snapcash (2014); Discovery, QR code incorporation, and facial recognition software (2015); Memories and Snapchat Groups (2016).

34. By 2015, advertisements were pervasive on Snapchat and, by 2018, 99% of Snap's total revenue came from advertising, according to internal company records. In other words, Snap decided to monetize its userbase and, from that point forward, began changing its product in ways that made its product even more harmful to users but that paved the way for growth, engagement, and profits for Snap and its leadership and investors.

35. The Snapchat product is best known for its self-destructing content feature. Snap's product allows users to form groups and share posts or "Snaps" that disappear after being viewed by the recipients. Snap emphasizes that everything you do on Snap disappears, and even notifies senders when someone takes a screenshot. These products and promises appeal to minor users, and encourage and allow minor users to exchange harmful, illegal, and sexually explicit images with adults. But also, these products provide predators with a safe and efficient vehicle to recruit victims. Snapchat is a go-to application for sexual predators because of these product features.[5]

36. Snap is widely accepted in the social media industry as having cornered the market on teen and tween engagement. It is the most popular social media product among tweens, teens, and young adults in the United States, and Snap works hard to market to and target this demographic – from product designs and features to commercials and merchandise to its logo. Snap's well-known logo is a ghost against a brightly colored background and some of the products for which it is best known include silly photo filters and bitmoji (cartoons).

[5] *See, e.g.*, https://phonespector.com/blog/what-are-the-dangers-of-snapchat-to-avoid/

37. Snap currently estimates more than 93 million Snapchat users in the U.S., including 17 million under the age of 18.

38. Snap claims that it does not provide its product to children under 13 or children under 18 without parental consent. However, Snap designs and operates its product in a manner that is intended to evade parental consent, does not provide parents with a 1-800 number or staffed email address to report unauthorized use by their children, and often does not stop distributing its product even when it knows or should know that parental consent is lacking.

39. For years Snap has received reports of child abuse and bullying occurring through its product and because of its product features,[6] yet has kept those features in place as removing them would impact the popularity of Snap's social media product. Harmful and dangerous interactions occur because of these and other Snapchat messaging features, which provide direct

[6] *See, e.g.*, https://www.forbes.com/sites/zakdoffman/2019/05/26/snapchats-self-destructing-messages-have-created-a-haven-for-child-abuse/?sh=411b8e1d399a (Snapchat Has Become A 'Haven for Child Abuse' With Its 'Self-Destructing Messages').

and unsupervised access to children and teens. But also, Snapchat does not operate as advertised. Snap's disappearing design and marketing of this feature is particularly harmful to teens who rely on Snap when taking and sending photos, only learning after the fact that recipients have means to save photos – and are often bullied, exploited, and/or sexually abused as a direct result.

40. Snap has developed images for users to decorate the pictures or videos they post. It has also developed Lenses which are augmented reality-based special effects and sounds for users to apply to pictures and videos users post on Snapchat, and World Lenses to augment the environment around posts. Snap also has acquired publication rights to music, audio, and video content that its users can incorporate in the pictures and videos they post on Snapchat. These images, Lenses, and licensed audio and video content supplied and created by Snapchat frequently make a material contribution to the creation or development of the user's Snapchat posts. Indeed, in many cases, the *only* content in a user's Snapchat post are images, Lenses, and licensed audio and video content supplied and created by Snapchat. When users incorporate images, Lenses, music, audio, and video content supplied by Snapchat posts, Snapchat makes a material contribution to the creation and/or development of their Snapchat postings and becomes a co-publisher of such content. When malign users incorporate images, Lenses, music, audio, and video content supplied by Snapchat to their posts, this enhances the psychic harm and defamatory sting that minor users experience from third-party postings on Defendant's platform.

41. Moreover, Snap contracts for legal rights in this third-party content, such that it is not "third-party content" at all. Snap's current Terms of Service grant Snap several, sweeping sets of legal rights, from licensing to ownership, as follows (and for example only as there are several provisions in Snap's Terms of Service that address legal rights over user content, comments, and other usage and activities),

//

//

//

//

> **3. Rights You Grant Us**
>
> Many of our Services let you create, upload, post, send, receive, and store content. When you do that, you retain whatever ownership rights in that content you had to begin with. But you grant us a license to use that content. How broad that license is depends on which Services you use and the Settings you have selected.
>
> For all content you submit to the Services, you grant Snap and our affiliates a worldwide, royalty-free, sublicensable, and transferable license to host, store, cache, use, display, reproduce, modify, adapt, edit, publish, analyze, transmit, and distribute that content. This license is for the purpose of operating, developing, providing, promoting, and improving the Services and researching and developing new ones. This license includes a right for us to make your content available to, and pass these rights along to, service providers with whom we have contractual relationships related to the provision of the Services, solely for the purpose of providing such Services.

Snap directly profits from the videos and pictures and other content its users create in collaboration with Snap, as described above.

C. Defendants Designed and Distributed Inherently Dangerous and/or Defective Products to Minors and Failed to Warn

42. Meta and Snap's social media products contain countless features that serve no critical purpose relating to product functionality or a user's ability to access other users' content. While this complaint addresses known features, on information and belief, there are countless other features currently unknown to Plaintiffs for the simple reason that these Defendants have concealed the truth and operate with zero transparency. Upon information and belief, it is in the public interest for this Court to permit discovery of all such product features and processes. The following describe just some such features and defective designs.

43. Meta and Snap design their products in a manner that results in evasion of parental consent and control.

44. Meta and Snap claim to impose age restrictions for use of their products, including that users must be at least 13 and must (or should, in the case of Meta) obtain parental consent if under the age of 18. Nevertheless, Defendants provide access to millions of minors under 13, or under 18 without parental consent and know or should know that these users are not authorized.

45. Meta and Snap also design product features that assist minor users in evasion of parental oversight and otherwise prevent parents from reasonable access to their children's activities. Snapchat's self-destructing content design feature is one example, with Meta having implemented a similar (though not default) feature in its Instagram product in late 2021. Defendants also do not restrict access by minors based on excessive or unhealthy use and do not notify parents concerning excessive, unhealthy, or other dangerous use, despite Defendants' actual tracking and knowledge of the same. Defendants do not notify parents when their children are contacted or solicited by adults; do not verify emails or phone numbers; do not prevent minors from opening multiple, secret accounts; and do not otherwise implement reasonable processes for enforcement of their stated age limitations and restrictions, or enforcement of other terms represented by Defendants as having been put in place for the safety of their users.

46. Meta and Snap also do not provide parents with an accessible, effective, and staffed reporting mechanism for unauthorized use by their minor children, and/or illegal or harmful activity. In short, when harms occur and are identified by parents, more often than not, those parents are then powerless to protect their children because of Meta and Snap's inadequate designs.

47. Meta and Snap offer limited in-app reporting features, which they do not explain or disclose to parents prior to use of their apps by minor children. But also, those in-app features require that parents either have access to their child's accounts, which often they do not, or their own accounts. Moreover, the in-app reporting mechanisms are defective and/or ineffective, and Meta does not respond to those reports in a manner designed to protect its minor users – as illustrated by Meta's lack of response and insufficient response to the harms at issue in this complaint.

48. Meta and Snap's public profile settings and product features – in place at all times relevant to this Complaint – are also inherently dangerous and/or defective when utilized in connection with minor users. Public profile and view settings allow strangers to view and message underage users and connect strangers with underage users, resulting in exploitation and abuse. Defendants have the ability to restrict minor accounts, set those accounts to private, limit the

information collected and disseminated/utilized in connection with those accounts, limit the use of recommendation technologies [product features] in connection with those accounts, and several other programming and/or product design changes Defendants could implement in a quick and cost-effective manner in order to better protect their minor users from these harms.

49. Meta and Snap's direct messaging and recommendation technologies are also inherently dangerous and defective when utilized in connection with minor users. Defendants direct-messaging products provide other users—including anonymous and semi-anonymous adult users, bullies, and other strangers for whom a parent would not allow access—with unrestricted and unsupervised access to minor users. Minor users lack the cognitive ability and life experience to identify online grooming behavior by prurient adults and the psychosocial maturity to decline invitations to exchange salacious material and mass-messaging capabilities. And again, there are several programming and/or product design changes Defendants could implement to protect their youngest users but choose not to as a matter of Defendants' cost-benefit analysis.

50. Lastly, Meta and Snap employ recommendation technologies, through which they affirmatively recommend and connect users to other users and/or groups. In Snap's case this is called "Quick Add," while Defendant Meta calls this "People You May Know" for its Facebook product and "Suggestions for You" for its Instagram product. These technologies function in a similar (if not the same) manner; specifically, Defendants' technologies/products utilize the extensive user data and information it collects from users to affirmatively direct users to one another in a manner intended to increase Defendants' own engagement and, thus, profits. Defendants' technologies/products push messages to users recommending that they connect, follow, friend, or otherwise, without regard to the risks caused by such affirmative connection efforts.

51. Meta, for example, has actual knowledge that its user recommendation technologies facilitate and contribute to most of the adult/minor grooming and exploitation that occurs on Meta's platform. Yet Meta has opted to continue utilizing those recommendation products anyway.

//

52. Each of the above-described products is dangerous alone but are substantially more dangerous when combined. For example, Defendants' direct-messaging products are more dangerous when coupled with minor accounts of which parents have no knowledge (or means to monitor) and do not consent; and when combined with Defendants' public profile and recommendation features.

53. Meta and Snap have purposely designed their products to be as addictive as possible and have actual knowledge of the harm these addictive features cause. Defendants knowingly or purposely designed their products to encourage addictive behaviors, for example,

a. Instagram is designed around a series of features that do not add to the communication utility of the application, but instead seek to exploit minor users' susceptibility to persuasive design and unlimited accumulation of unpredictable and uncertain rewards. Examples of this include but are not limited to "likes," "followers," algorithm-controlled feed, and unlimited scrolling features.

b. Snapchat features a series of rewards including trophies, streaks, and other signals of social recognition. These variable and unknown reward and reminder systems are particularly addictive, especially in the case of children and teens. Other product examples include recommendation technologies and unlimited scrolling features.

54. These product features serve no purpose other than creating dependencies on Meta and Snap's products by children and teens, resulting in sleep deprivation, anxiety, depression, anger, shame, interpersonal conflicts, and other serious harms to mental and physical health.

55. Meta and Snap also send push notifications and emails to encourage addictive behavior and to increase use of their social media products. Defendants' communications are triggered and based upon information collected from and about their users, and Defendants "push" these communications to teen users in excessive numbers and at disruptive times of day. These notifications are specifically designed to, and do, prompt them to open Defendants' social media

products, resulting in greater profits to Meta and Snap.

56. These are just known examples, and Plaintiffs believe that they will identify other examples of harmful product features through discovery in this case.

57. But also, Meta and Snap have each developed artificial intelligence technology that detects adult users who send sexually explicit content to children and receive sexually explicit images from children. These technologies furnish Meta and Snap with actual knowledge that a significant number of minor users of their products are solicited to send, and do send, sexually explicit photos and videos of themselves to adult users in violation of 18 U.S.C. § 1591(a)(1)-(2). Meta and Snap *could* protect their minor users, but in many instances, do not.

D. Defendants' Social Media Products are Products

58. Instagram and Snapchat are products that are designed and manufactured by Meta and Snap respectively. These products are designed to be used by children and are actively marketed to children throughout the world.

59. Meta and Snap make and distribute Instagram and Snapchat, respectively, with the intent that they be used and consumed by the public as part of Meta and Snap's regular business.

60. Meta and Snap design Instagram and Snapchat to be used by minors and actively market Instagram and Snapchat to minors across the United States.

61. Meta and Snap refer to their social media products and product features as "products," and designate them as products when it is to their benefit to do so.

E. Defendants' Business Model is Based on Maximizing User Screen Time

62. Meta and Snap advertise their products as "free" because they do not charge their users for downloading or using their products. What many users do not know is that, in fact, Meta and Snap make a profit by finding unique and increasingly dangerous ways to capture user attention and target advertisements to their users. Meta and Snap receive revenue from advertisers who pay a premium to target advertisements to specific demographic groups of users in the applications. Meta and Snap also receive revenue from selling their users' data to third parties.

//

63. The amount of revenue Meta and Snap receive is based upon the amount of time and level of user engagement on their platforms, which directly correlates with the number of advertisements that can be shown to each user.

64. Meta and Snap use unknown and changing rewards that are designed to prompt users who consume their social media products in excessive and dangerous ways. Meta and Snap know, or in the exercise of ordinary care should know, that their designs have created extreme and addictive usage by minor users, and Meta and Snap knowingly design their products to encourage such addictive behaviors. This design conforms to well-established principles of operant conditioning wherein intermittent reinforcement provides the most reliable tool to maintain a desired behavior over time.

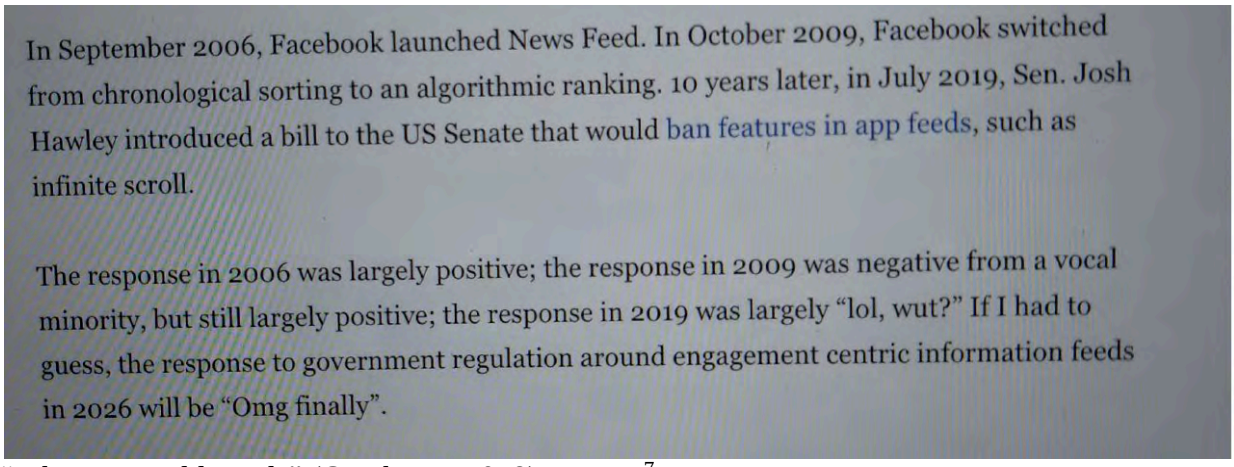
65. Instagram and Snapchat are designed around a series of features that do not add to the communication utility of the application, but instead seek to exploit minor users' susceptibility to persuasive design and unlimited accumulation of unpredictable and uncertain rewards, including "likes" and "followers." In the hands of children, this design is unreasonably dangerous.

66. According to industry insiders, Meta and Snap have employed thousands of psychologists and engineers to help make their products maximally addicting; to keep users, and particularly young users, engaged longer and coming back for more. This is referred to as "engineered addiction," and examples include features like bottomless scrolling, tagging, notifications, live stories, and "pull to refresh" features (based on how slot machines operate, this creates an endless feed, designed to manipulate brain chemistry, and prevent natural end points that would otherwise encourage users to move on to other activities).

67. Meta and Snap know that their products are addictive, and that millions of teen users want to stop using them but cannot.

68. Meta and Snap have also designed their products to maximize users' screen time by using complex algorithms designed to exploit human psychology and driven by the most advanced computer algorithms and artificial intelligence available to some of the largest technology companies in the world.

69. Meta and Snap's recommendation systems select potential contacts and content for minor users not based on what they anticipate the user will prefer or to enhance their social media experience, but rather for the express purpose of habituating users to Meta and Snap's social media products. In the words of one, high-level departing Meta employee:


In September 2006, Facebook launched News Feed. In October 2009, Facebook switched from chronological sorting to an algorithmic ranking. 10 years later, in July 2019, Sen. Josh Hawley introduced a bill to the US Senate that would ban features in app feeds, such as infinite scroll.

The response in 2006 was largely positive; the response in 2009 was negative from a vocal minority, but still largely positive; the response in 2019 was largely "lol, wut?" If I had to guess, the response to government regulation around engagement centric information feeds in 2026 will be "Omg finally".

"Why We Build Feeds" (October 4, 2019), at p. 1.[7]

70. Meta and Snap have designed algorithm-controlled product features to promote content and connections most likely to increase user engagement, despite their knowledge that content that generates extreme psychological reactions in minor users is more likely to trigger their engagement than content that is benign. Defendants expose users to significant amounts of content and connections that they would never see and/or meet but for Defendants' products and designs, including content and connections that are inherently harmful to minor users' health.

F. Minor Users' Incomplete Brain Development Renders Them Particularly Susceptible to Manipulative Social Media Products with Diminished Capacity to Eschew Self-Destructive Behaviors and Less Resiliency to Overcome Negative Influences

71. The human brain is still developing during adolescence in ways consistent with the demonstrated psychosocial immaturity of adolescents. Specifically, adolescents' brains are not yet fully developed in regions related to risk evaluation, emotional regulation, and impulse control.

72. The frontal lobes—and in particular the prefrontal cortex—of the brain play an essential part in higher-order cognitive functions, impulse control, and executive decision-making.

[7] https://www.documentcloud.org/documents/21600853-tier1_rank_exp_1019

These regions of the brain are central to the process of planning and decision-making, including the evaluation of future consequences and the weighing of risk and reward. They are also essential to the ability to control emotions and inhibit impulses. MRI studies have shown that the prefrontal cortex is one of the last regions of the brain to mature.

73. During childhood and adolescence, the brain is maturing in at least two major ways. First, the brain undergoes myelination, the process through which the neural pathways connecting different parts of the brain become insulated with white fatty tissue called myelin. Second, during childhood and adolescence, the brain is undergoing "pruning"—the paring away of unused synapses, leading to more efficient neural connections. Through myelination and pruning, the brain's frontal lobes change to help the brain work faster and more efficiently, improving the "executive" functions of the frontal lobes, including impulse control and risk evaluation. This shift in the brain's composition continues throughout adolescence and into young adulthood.

74. In late adolescence, important aspects of brain maturation remain incomplete, particularly those involving the brain's executive functions and the coordinated activity of regions involved in emotion and cognition. As such, the part of the brain that is critical for control of impulses and emotions and for mature, considered decision-making is still developing during adolescence, consistent with the demonstrated behavioral and psychosocial immaturity of juveniles.

75. The technologies in Meta and Snap's social media products are designed to exploit the diminished decision-making capacity, impulse control, emotional maturity, and psychological resiliency of minor users caused by incomplete brain development. Meta and Snap know that because their minor users' frontal lobes are not fully developed, they experience enhanced dopamine responses to stimuli on Meta and Snap's social media platforms and are therefore much more likely to become addicted to Meta and Snap's products; exercise poor judgment in their social media activity; and act impulsively in response to negative social media encounters. Meta and Snap also know, or in the exercise of reasonable care should know, that minor users of their social media products are much more likely to sustain serious physical and psychological harm through their social media use than adult users.

76. Nevertheless, Meta and Snap designed their social media products to be addictive to minor users and failed to include safeguards to account for and ameliorate the psychosocial immaturity of their minor users.

G. Defendants Misrepresent the Addictive Design of Their Social Media Products

77. Meta and Snap do not warn users of the addictive or harmful design of their products. On the contrary, they consistently play down their products' negative effects on teens in public statements and advertising but then refuse to make their research public or available to academics or lawmakers who ask for it.

78. During the relevant time period, Meta and Snap represented to the public and governments around the world that their products were safe and not addictive, and not designed to be addictive. Defendants knew or should have known that their statements were false or materially misleading.

79. During the relevant time period, Meta and Snap advertised via commercials and/or third parties that their products were fun and safe to use, age-appropriate for children as young as 12+, and that they employed their technologies to protect minor users from harm. Defendants knew or should have known that their statements were false or materially misleading.

80. Meta and Snap did not warn users or their parents of the addictive and mentally harmful effects that the use of their products was known to cause amongst some minor users.

81. Meta and Snap did not warn users or their parents of the harms certain of their product features cause, particularly to minor users, such as public profile settings, unrestricted direct messaging, anonymous or semi-anonymous profiles, user recommendations, and similar.

H. Plaintiffs Disclaim Any and All Claims Seeking to Hold Defendants Liable as the Publisher or Speaker of Any Content Provided, Posted, or Created by Third Parties

82. Plaintiffs seek to hold Meta and Snap accountable for their own alleged acts and omissions. Plaintiff's claims arise from Meta and Snap's status as designers, distributors, and marketers of defective social media products, as well as Meta and Snap's own statements and actions, and failures to warn and act, and not as the speaker or publisher of third-party content.

//

83. Meta and Snap designed and have progressively modified their products to promote problematic and excessive use that they know is indicative of addictive and self-destructive use. Meta and Snap's product features are addictive and harmful without regard to any content that may exist on Defendants' platforms.

84. Meta and Snap have designed other product features that encourage and assist children in evasion of parental oversight, protection, and consent, which features are wholly unnecessary to the operation of their products and are harmful without regard to any content that may exist on Defendants' platforms.

85. Meta and Snap's products identify minors and collect a myriad of personal and device data points from those minors, both on and off their platforms, then use those extensive data points to direct specific content and connections to minors aimed at increasing minor user engagement with their social media products. These technologies and Defendants' design, operation, and programming of the same affirmatively direct harmful content and predatory adult users to Defendants' vulnerable minor users, which harms Defendants know or should know about.

86. Meta and Snap are responsible for these harms, which are caused by Defendants' designs and design-decisions, not any third party or third-party content. Indeed, while it may be that a third party creates a particular piece of harmful content, the teens and children harmed by Meta and Snap's social media products are not being harmed by a single piece of harmful content. They are being harmed by Meta and Snap's products, programming, and decisions to continue exposing teens and children to harmful product features in the name of engagement.

87. None of Plaintiff's Claims for Relief set forth herein treat Meta and Snap as a speaker or publisher of content posted by third parties. Rather, Plaintiffs seek to hold Meta and Snap liable for their own speech and their own silence in failing to warn of foreseeable dangers arising from anticipated use of their products. Defendants could manifestly fulfill their legal duty to design a reasonably safe social product and furnish adequate warnings of foreseeable dangers arising out of the use of their products without altering, deleting, or modifying the content of a single third-party post or communication. Some examples include,

//

a. Prioritizing internally their existing programming when it comes to content pushed to users as well as enforcement of their own terms of service and community standards.

b. Requiring identification upon opening of a new account and parental consent for users under 18 (which Snap currently claims to do but does not actually enforce) and restricting users under 18 to a single account.

c. Email and phone number verification when any user opens a new account.

d. Setting all minor accounts to private, and not allowing public profiles for any person under the age of 18.

e. Limiting the types of data collected from minor users and not utilizing user, group, or content recommendation technologies on minor accounts, and otherwise limiting direct messaging products with any user under 18.

f. Decreasing the speed of their recommendation technologies on minor accounts and restricting access for minors to addictive product features.

88. These are just some examples, all of which could be accomplished easily and/or at commercially reasonable cost and all of which can be accomplished by Defendants unilaterally and without regard to third party content.

V. PLAINTIFF-SPECIFIC ALLEGATIONS

89. John Doe currently is only 15 years old.

90. He is a mature, respectful, and upbeat person, who enjoys playing sports and is well-liked by his teachers and friends.

91. John Doe opened his first Instagram account when he was only 10 years old, and he did so without his father's knowledge or consent. Meta undertakes no reasonable effort to verify age or parental consent and makes its social media product available to minors in a way that makes it impossible for parents to prevent such access – even when they try.

92. Specifically, in October of 2017, John Doe went on a trip to Japan with his grandparents. His grandfather provided him with a cell phone upon arriving in Japan. One day later, John Doe opened his first Instagram account, without his parent or grandparents' knowledge

or consent. He was underage, which fact Meta knew or should have known based on his Instagram activity and/or data Meta routinely collects from users, including information that informs Meta of each user's estimated actual age. Meta allowed him to use the account regardless.

93. A.C. only discovered the account because John Doe commented on an Instagram post published by someone who knew A.C., and who notified A.C. of his son's account. Upon John Doe's return from Japan the phone was confiscated and put in A.C.'s room for safe keeping, and John Doe was told that he could not use Instagram. Again, however, Meta takes no reasonable steps to confirm parental knowledge and consent, making it easy for underage children to continue using its social media product.

94. John Doe began sneaking into his father's room and would use the phone to access Instagram then put it back when he was done. John Doe was a good kid, and never gave his father reason to mistrust him; however, and like many kids, his growing desire to continue using the Instagram product caused him to act in uncharacteristic ways.

95. One day in 2018, John Doe snuck into his father's room only to find that the phone was no longer there. This also did not prevent him from accessing Instagram. Instead, he began using his computer and continued to use Instagram without his father's knowledge or consent.

96. Accessing Instagram via computer was not the same, however, so John Doe began looking for solutions. In November 2018, he used a Visa gift card he had received (likely for his birthday) to purchase a Samsung Galaxy S Blaze from eBay. But the Instagram app wouldn't update on that phone, so he used a gift card to purchase an LG Ultimate 2, also on eBay, and kept the device hidden from his father. A.C. had no idea this was happening, while Meta did – at least, the details of each new device and each new Instagram download are among the data points Meta collects from every user every time an account is accessed.

97. John Doe also accessed Instagram on a family device used for Pokémon GO. This was a device A.C. had purchased to replace his aging personal phone, but he was unhappy with the quality of the camera, so he disconnected the phone service, and they began using the device to play Pokémon GO together. On one occasion, he allowed John Doe to take the phone to a sleepover, on the condition that he would use it to play Pokémon GO only. While his father had

no reason to mistrust him, it now appears from Meta's data that John Doe accessed his Instagram account on that Wi-Fi accessible device on that one occasion as well.

98. When A.C. discovered John Doe's secret phone, they discussed the situation. John Doe already understood that his purchase and use of a phone without his father's permission was wrong, but also, they discussed why it was so important for his parent to be aware of what he was doing and for him to obtain parental permission and to keep his word. John Doe was not allowed to keep using the secret phone.

99. It was not until late 2018 when John Doe got his own cell phone. He and his father discussed responsibility, the need for a device that could actually make and receive phone calls, and the importance of using that device with A.C.'s permission and in ways of which he approved. John Doe was not allowed to have an Instagram account. However, he began using his new cell phone for Instagram in March of 2019 and added his number to his Instagram account in July of 2020. John Doe was once again using Instagram without his father's knowledge or consent.

100. In late 2019, A.C. realized that John Doe was using Instagram. More to the point, he realized that he could not physically stop John Doe from using Instagram or Meta from distributing its product to his son. Meta made no reasonable effort to verify age or parental consent and made its product available to children on all manner of electronic devices, which devices are everywhere. He also understood that John Doe was using Instagram to browse photos and videos and to communicate with his friends. Under the circumstances, the only way A.C. could help protect his son was to exercise parental control and oversight in his son's use of Instagram.

101. A.C. did not consent to John Doe using Instagram, but Meta had no reporting or protection mechanism to prevent such use. A.C. understood, based on Meta marketing and reputation, that the biggest concern with Instagram was posting of potentially embarrassing content and kids being mean to one another. For these reasons, he talked with his son about taking care in comments made to others, he required access and reviewed John Doe's account and communications and prohibited him from publishing posts. Ultimately, A.C. had no means to enforce these rules and now knows that John Doe did not always follow them.

//

102. By early 2020, John Doe was allowed to publish posts as long as he first obtained A.C.'s review and approval – which he did, for the most part. In January of 2021, A.C. opened his own Instagram, in the hopes that he could obtain a better sense of his son's use and activities. Eventually, he allowed John Doe to post without first seeking approval, based on his track record of trustworthiness in this regard and because, with his own account, A.C. was receiving a notification each time his son posted and was able to then review.

103. Like Meta, Snap also designs and distributes its product in a manner that allows minors to use the Snapchat product without parental knowledge or consent.

104. A.C. does not know when John Doe opened his first Snapchat account and only learned that John Doe had a Snapchat account *after* the events in this complaint took place. John Doe opened that account without his father's knowledge or consent.

105. John Doe's use of Instagram and Snapchat resulted in his exploitation, and caused and/or worsened depression, anxiety, and obsessive behaviors – which harms were not just foreseeable by Meta and Snap but have been identified by Defendant Meta as among the types of harms use of its social media products cause for a significant number of minor users.

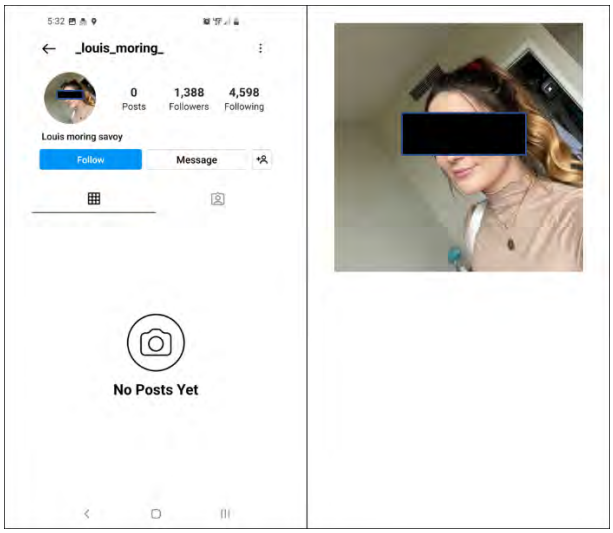
106. On May 10, 2022, Instagram user **_louis_moring_** connected with minor user John Doe via Meta's product features, including the Suggested for You and/or public profile features. **_louis_moring_** did not know John Doe in real life and would never have found him but for decisions Meta made over the last several years with regard to its product design and distribution. **_louis_moring_** likewise would not have been able to initiate direct and unsupervised contact with minor John Doe but for those Meta decisions.

107. Instagram user **_louis_moring_** began by following John Doe's Instagram account. John Doe was generally cautious, based on discussions with his father, and removed people he did not recognize or know in real life. This is what he did with **_louis_moring_**, only for that user to re-follow him quickly thereafter and then engage with him via Meta's direct message product.

108. **_louis_moring_** posed as a young, female user at all times relevant.

109. John Doe asked if he knew her, and she replied by expressing sexual interest in him. John Doe was a 14-year-old boy and was predictably responsive to **_louis_moring_**'s

overtures. Moreover, **_louis_moring_** had more than a thousand followers on Instagram, conveying that she was an established and trustworthy user who had not been reported to Instagram, was not a catfish, and was someone he could trust. **_louis_moring_** began sending him provocative photos and videos and asked him to send provocative photos and videos in return.



110. John Doe was reluctant to send photos of himself at first, even after **_louis_moring_** purported to send photos and videos of "herself." Then the suggestion of Snapchat came up, and John Doe agreed and shared his Snapchat username with **_louis_moring_**. John Doe believed that he could safely share such content on Snapchat because of Snap's disappearing content features. He knew that this was something kids his age used Snapchat to do, and reasonably believed that there was little to no risk as long as he sent the content via Snapchat.

111. On May 11, 2022, John Doe used the Snapchat product to send three illicit photos and two illicit videos to the user who contacted him via Instagram, with the understanding and belief that this was a relatively safe way to send such content since it would disappear once viewed. Instead, the user – a complete stranger to minor John Doe – sent him back a collage of his photos, via the Snapchat product, and told him that if he did not pay them immediately they would be sharing the three illicit photos and two illicit videos of John Doe to his family and friends. John Doe did not know that others could capture his content and is still not certain as to how **_louis_moring_** was able to do so given how the Snapchat product is advertised by Snap.

//

112. John Doe's Instagram and Snap profiles were publicly viewable when **_louis_moring_** found him, which both Defendants previously utilized as account defaults even on minor accounts. But for public profile and viewability settings, **_louis_moring_** would not have been able to find John Doe in the first place and would not have been able to see and take note of all of John Doe's "friends" on the two social media products, and even "friends" of "friends." These are inherently dangerous settings, particularly when it comes to minors like John Doe

113. But also, these two social media products – Instagram and Snapchat – work together to amplify and exacerbate the harm. A common pattern among predators is to use Instagram's public profile and recommendation features and settings to find minors to exploit, then convince those children to either provide their Snapchat username to them or open a Snapchat account to enable such exploitation in what adult and minor users believe to be a risk-free environment.

114. John Doe attempted to block the user from his Snapchat account, so **_louis_moring_** reached back out to him via direct message on his Instagram account.

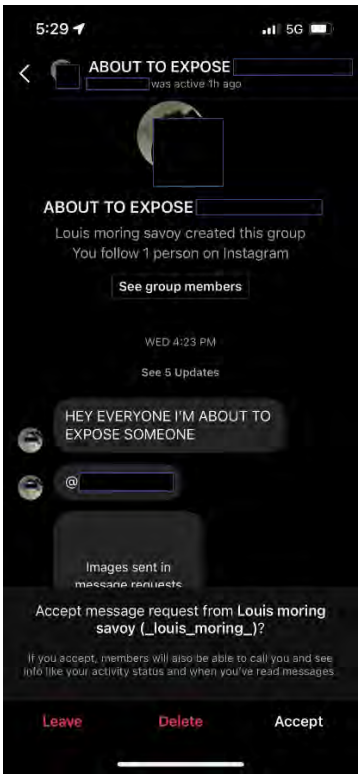
115. On May 11, 2022, **_louis_moring_** used Meta's product features to start a Group Chat, which they titled "ABOUT TO EXPOSE [John Doe]" while repeatedly sending direct message threats to then 14-year-old John Doe that if he did not pay immediately his photos and videos would be published to friends and family.

116. From May 11 through May 13, 2022, John Doe tried changing his Instagram username, blocking **_louis_moring_** from his Instagram account, changing his profile text, changing his profile settings to private, and anything else he could think to protect himself – but nothing worked. That is simply not how Meta's products are designed; Meta's products prioritize user engagement at the expense of user safety.

117. No matter what John Doe did, **_louis_moring_** got through to him using Defendants social media products and product features and made their intention clear, and then 14-year-old John Doe suffered greatly as a result.

118. Then **_louis_moring_** began adding people John Doe knew in real life to the Group Chat "she" created on Instagram, and where "she" had published his intimate photos and videos. This content was taken of then 14-year-old John Doe and, as such, constitutes Child Sexual Abuse

Material (CSAM) and publication of that material was illegal in multiple regards.



119. A.C. had no way of knowing what was happening to his own child under his own roof because of the Instagram and Snap social media products; but they spent every day together and A.C. knew that something was wrong. He noticed a change in John Doe's mood starting on May 11, 2022. John Doe was normally upbeat, chatty, and happy, but had become distracted, bothered, and withdrawn. He was no longer interested in talking about his favorite sports or engaging in conversation.

120. A.C. attempted to check in with John Doe and asked if he was okay.

121. On May 14, 2022, A.C. asked John Doe if there was something going on that he did not know about, and John Doe said "yes." A.C. asked if he wanted to talk about it, and John Doe said "no." However, when A.C. asked whether John Doe would be okay, John Doe said "I don't know," which is when A.C. knew that he couldn't simply let it go. After several more questions and well-placed concern, John Doe finally told his father everything and A.C. immediately set out to help protect his son – not just from **_louis_moring_** but also from the harms Snap's product already had caused and Meta's product was still causing to his son.

122. **_louis_moring_** was just one "person," who did not know John Doe and could not have done anything to hurt John Doe but for Meta and Snap's products, failures to warn, and failures to provide any sort of reasonable safety features or reporting and enforcement mechanisms. Meta and Snap made it possible for that stranger to exploit and threaten A.C.'s son, publish illicit and illegal content, seemingly without recourse, harass John Doe via private message features, find and then harass John Doe's friends and family and even *their* friends and family, and otherwise perpetrate these harms. Meta and Snap never should have provided John Doe with access to their products in the first place, and now A.C. needed to find a way to report and stop the harm that was being caused.

123. Only, as A.C. soon learned, Meta and Snap also designed their products in a manner that makes the successful reporting and the protection of minors all but impossible.

124. First, A.C. researched the Instagram product. He read every article he could find to try to stop what was happening. When that didn't help, he started looking for information on Meta's direct message and Group Chat features, then read through every Meta "Support" document he found and scoured Meta's sites and the internet at large to find a Meta support number he could call to report what was happening – no such number existed, and nothing he found told him how to stop what was happening. Meta provided no phone number or monitored email address for reporting, and no immediate response mechanism, no matter how serious the harm. Meta did not even provide a button minor users can use to report exploitation and harm occurring because of the platform in order to obtain immediate help from Meta, despite representing in its terms to users that it utilizes its technology to keep them safe. A.C. had no way to report the illicit images of his minor child or get them taken down. He could not even stop them from being published and copied countless times via Meta's servers, which is precisely what was happening.

125. The most A.C. could do was to navigate to the **_louis_moring_** account and select a report account option (which had to be done from an existing Instagram account – which thankfully he had) and hope Meta received and acted on it immediately. Even then, A.C. could only select from one of a number of pre-designated reporting descriptions, without any option for direct contact with a Meta representative or any way to provide additional information.

126. On May 14, 2022, A.C. reported the **_louis_moring_** account via John Doe's account and his own, requested and downloaded an export of all content and data from John Doe's account, then deleted John Doe's account and uninstalled the Instagram app in the hopes that he could stop what Instagram was allowing.

127. On May 15, 2022, A.C. asked another Instagram user, whose name he had seen in the Group Chat before having taken the steps above, to check their Instagram account. The Group Chat was not only still there – it now included more than 17 people, most of whom knew A.C. and John Doe in real life and many of whom were John Doe's classmates and friends (who also are minors). A.C.'s report to Meta appeared to have done nothing.

128. 24 hours passed, and Meta had yet to take any action with regard to the **_louis_moring_** account, as that account was still up and active – and actively causing harm to John Doe and A.C.

129. May 15 was a Sunday. A.C. spent it with his son to make sure he was okay. They talked about how to handle school the next day. They came up with a plan in case things went bad and John Doe needed his father to come get him. They talked about what could happen, and how things might be okay.

130. A.C. did everything he could to protect his son – including from the harm John Doe might suffer and/or cause himself because of Meta's failure to act on A.C.'s report. A.C. was extremely concerned and wanted to know that John Doe was not going to hurt himself.

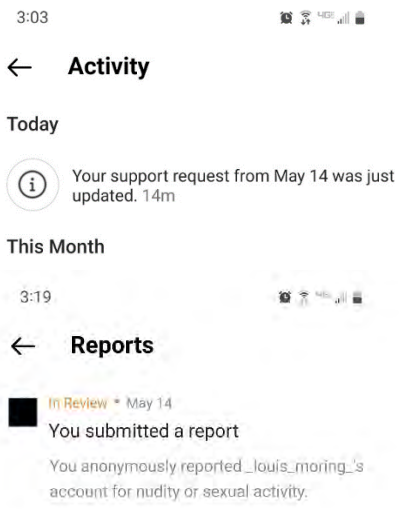
131. On May 16, John Doe went to school and made it through the day.

132. Since making his report on May 14, A.C. had not stopped checking Instagram in the hopes that Meta had taken some action to protect his son from the known and ongoing harm that was snowballing out of control because of its social media product. On May 17, he received a notification from Meta on his Instagram app and, when he opened the app on his Android, it simply said that his report was still "In Review." A.C. was distraught and devastated.

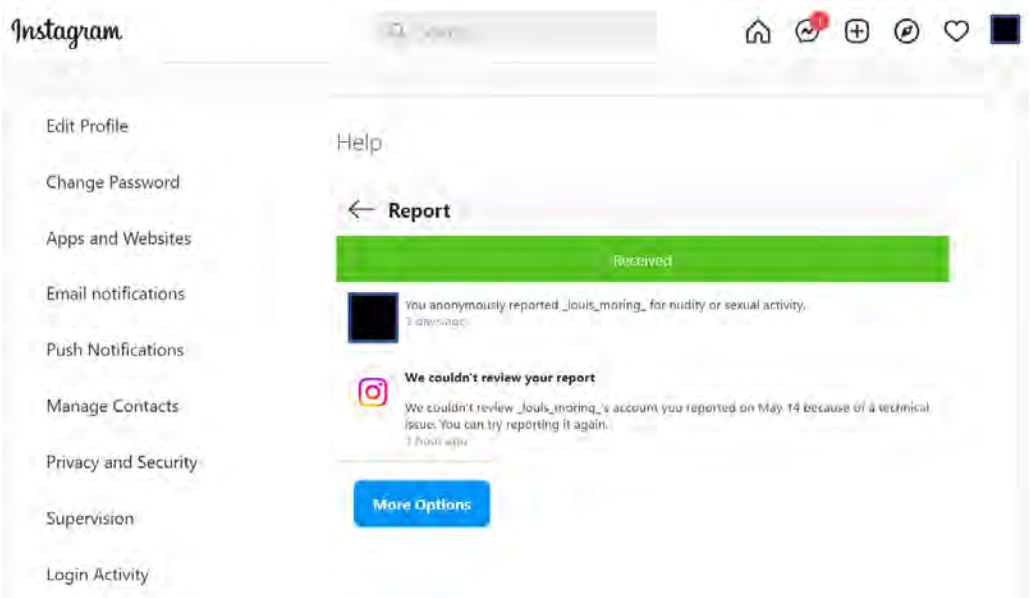
//

//

//



133. A.C. immediately checked the **_louis_moring_** account and was distressed to find it still active. Shortly thereafter he checked Instagram again, this time from his computer via the Firefox web browser, and this time he got the message that Meta could not review his report due to a technical issue. Meta suggested that he try reporting **_louis_moring_** again.



134. To be clear, this was not an update but, in fact, Meta responded to the same report A.C. had submitted in two different ways, depending on how A.C. accessed his Instagram account. These responses reflect a fundamental defect in Meta's reporting mechanisms, and this was not the only time that this defect resulted in harm to Plaintiff A.C. and his son.

//

135. A.C. works with computers and technology for a living, and quite literally could not get through to anyone at Meta and could not get Meta to take down the CSAM it was hosting or to otherwise stop the incredible harms it was causing to his then 14-year-old son.

136. At this point, A.C. had been trying everything for more than three days, anxiously waiting for Meta to act and constantly worrying about his son's safety and well-being. He knew that his son's intimate photos and videos were accessible to his classmates and others, and he could not even get Meta – arguably the most sophisticated tech company in the world – to review the offending account due to what Meta claimed to be a "technical issue."

137. In the meantime, Meta continued to earn revenue from the **_louis_moring_** account and all of the related account activity described above.

138. Up to this point, A.C. had researched every Instagram report option and support form and had followed Meta's instructions precisely. As required by Meta he did not report the Instagram user multiple times from a single account and did not falsely answer a question on any report form available on the Instagram website (and in answering the questions honestly *there was no form he could submit*). So, on May 17, 2022, A.C. went back to Meta's Help Center.

139. Meta's Help Center provided two web forms for reporting content/accounts, (1) Report Harassment or Bullying on Instagram and (2) Report Violations of Our Community Guidelines. A.C. then tried to submit reports through these mechanisms, but when attempting to file a report using either form (and answering the questions honestly), one of the four following events occurred,

a. Meta presented a message stating that if you have an Instagram account "you can report a photo or video from within the app." And the form discontinued or became disabled.

b. Meta presented a message stating that "If you're not able to view the content you need to report, please have a friend copy and send you the link. Then, come back here to report it. Note: You won't be able to submit this form unless you have the link to the abusive content." And the form discontinued or became disabled.

c. The Meta form presented a field requiring a link to the content being reported in order to submit the form (which doesn't exist in the case of abusive photos or messages within a Group Chat).

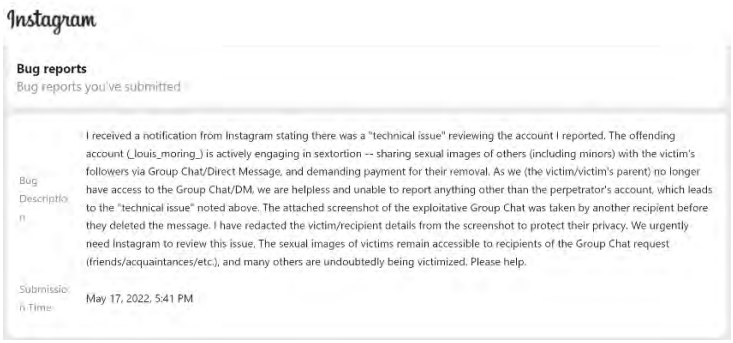
d. The webpage immediately, unexpectedly, and for no apparent reason, redirected to a generic, unrelated help page (taking him away from the form).

140. Being a web developer, A.C. tried completing the forms Meta provided when logged in and out of Instagram, from different web browsers, devices, and network connections, to ensure that the outcome was not unique to him. It wasn't. The barrier was with Meta alone, evidencing additional product defects and resulting in more harms to A.C. and his son.

141. At this point, A.C. again reported the **_louis_moring_** account from within the Instagram app. Sensing that this was a dead end, he searched for any possible means of getting someone (anyone) at Meta to see the details of the harms that were taking place. He took the following three actions.

142. First, he reported the details of what was happening and the "technical issue" via the "Report a Problem" feature in the Instagram app (intended for reporting technical bugs, not abuse). His report read:

> I received a notification from Instagram stating there was a "technical issue" reviewing the account I reported. The offending account **(_louis_moring_)** is actively engaging in sextortion – sharing sexual images of others (including minors) with the victim's followers via Group Chat/Direct Message and demanding payment for their removal. As we (the victim/victim's parent) no longer have access to the Group Chat/DM we are helpless and unable to report anything other than the perpetrator's account, which leads to the "technical issues" noted above. The attached screenshot of the exploitative Group Chat was taken by another recipient before they deleted the message. I have redacted the victim/recipient details from the screenshot to protect their privacy. We urgently need Instagram to review this issue. The sexual images of victims remain accessible to recipients of the Group Chat request (friends/acquaintances/etc.) and many others are undoubtedly being victimized. Please help.


Instagram

Bug reports

Bug reports you've submitted

Bug Description

I received a notification from Instagram stating there was a "technical issue" reviewing the account I reported. The offending account (_louis_moring_) is actively engaging in sextortion -- sharing sexual images of others (including minors) with the victim's followers via Group Chat/Direct Message, and demanding payment for their removal. As we (the victim/victim's parent) no longer have access to the Group Chat/DM, we are helpless and unable to report anything other than the perpetrator's account, which leads to the "technical issue" noted above. The attached screenshot of the exploitative Group Chat was taken by another recipient before they deleted the message. I have redacted the victim/recipient details from the screenshot to protect their privacy. We urgently need Instagram to review this issue. The sexual images of victims remain accessible to recipients of the Group Chat request (friends/acquaintances/etc.), and many others are undoubtedly being victimized. Please help.

Submission Time

May 17, 2022, 5:41 PM

He included a screenshot of the Group Chat with the "bug report" submission.

143. Second, he again reported the **_louis_moring_** account, via the "Report Violations of Our Community Guidelines" web form, selecting that he did not have an Instagram account, which was the only method of actually submitting details via either form.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

Submitted from: Instagram Website Form

Submission details were as follows:

Do you have an Instagram account?
Selection: No

Where does the violation you're reporting appear?
Selection: An entire profile

How is this profile violating our guidelines?
Selection: Nudity or pornography

Your Instagram username (if applicable):
[redacted]

Your email address:
[redacted]

Username of the person who posted the content you are reporting:
_louis_moring_

Full name of the person who posted the content as listed on their account (optional):
Louis moring savoy

Username(s) of the profile(s) you are reporting
_louis_moring_

Do you know this person in real life?
No.

Additional information:

The offending account (_louis_moring_) is actively engaging in sextortion -- sharing sexual images of others (including minors) with the victim's followers via Group Chat/Direct Message, and demanding payment for their removal.

This is in direct violation of Instagram's policies: "We have zero tolerance when it comes to sharing sexual content involving minors or threatening to post intimate images of others."

As we (the victim/victim's parent) no longer have access to the Group Chat/DM, we are helpless and unable to report anything other than the perpetrator's account.

We urgently need Instagram to unsend/delete Group Chats/DMs created by the "_louis_moring_" user and terminate their account (after an appropriate review, of course). While we wait, the sexual images of victims remain accessible by recipients, and many others are undoubtedly being victimized/extorted. Please, please help. Thank you.

144. Third, he replied to the auto-response email he received from Meta after completing the report web form with further details and screenshots. Here is the auto-response Meta sent

//

//

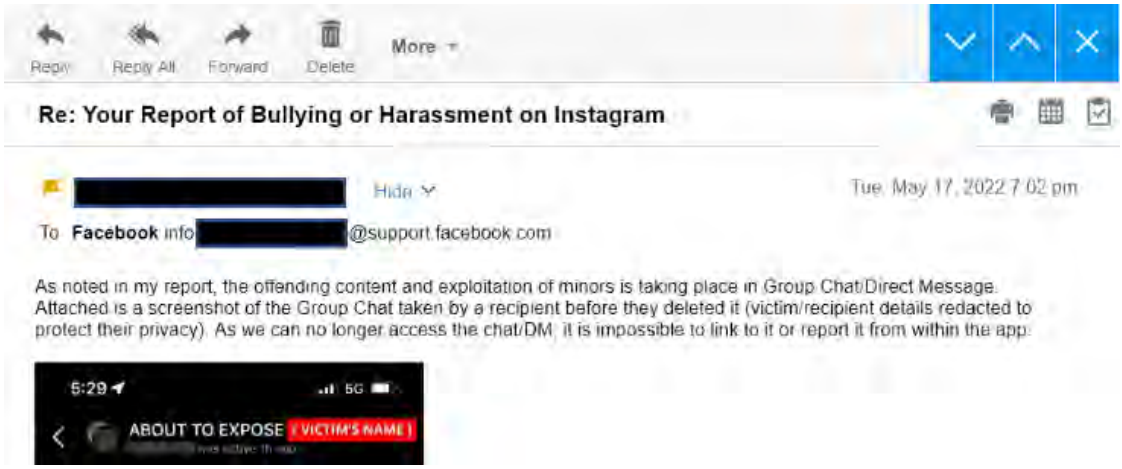
//

//

On Tue, May 17, 2022 at 6:26 PM, Facebook <info[redacted]@support.facebook.com> wrote:

> Hi,
>
> Thanks for contacting us. We've received your report and will review it in the order in which it was received.
>
> We require specific pieces of information in order to take action on your report:
> - A link to the content you're reporting
> - The username of the abusive profile
> - A description of how the content is abusive
>
> If you didn't previously provide us with this information, please do so now by responding to this message. Though you may not receive any further response from us, we are reviewing your report and will take the appropriate action based on our Terms.
>
> Keep in mind that you can always block someone if you don't like what they're sharing on Instagram:
> http://help.instagram.com/454180787965921?ref=cr
>
> You can also change your profile's visibility to private:
> https://help.instagram.com/448523408565555?ref=cr
>
> Thanks,
> The Instagram Team

And here is the response A.C. sent back to Meta,



145. On May 18, A.C. continued to monitor the **_louis_moring_** account and check his reports and emails for any status update from Meta.

146. Finally, on Wednesday, May 18, 2022, the **_louis_moring_** Instagram profile web page showed "Sorry, this page isn't available." It took Meta several days and countless reports to presumably take down a predator user – though A.C. could not even be certain that Meta had taken down the account. A.C. also had no way to know or confirm whether the Group Chat and exploitative photos and videos of his son were still accessible to others.

147. Moreover, A.C. never received confirmation from Instagram that the **_louis_moring_** account had in fact been removed. A.C. searched himself for any means to

confirm that the account was removed (as opposed to the account holder changing its username or temporarily disabling the account) and discovered that none exists. Further, when he checked on May 18, 2022, via the Instagram app, he had the same "In Review" message for his reports of **_louis_moring_** made May 14 and May 17.

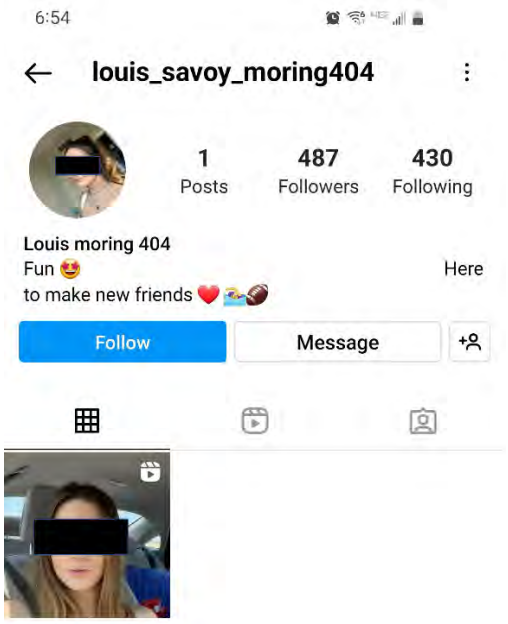
148. A.C. continued to actively monitor the report status and *to this day* – almost five months after he made the first report – his Instagram app still states that the reports are "In Review."

149. In the meantime, A.C. could not be certain whether the account was removed; was aware that there was still a chance that the Group Chat containing his son's illicit photos and videos still existed and was accessible to an unknown number of people; was aware that the perpetrator was still in possession of his son's photos and videos, and could continue distributing and publishing them; and was painfully aware that the perpetrator was surely victimizing other children while Meta refused to act on knowledge in its actual possession (several times over).

150. A.C. became distraught and emotionally distressed as a direct and proximate result and proceeded to monitor Instagram daily in the coming weeks. No matter what he did, he could not get through to anyone at Meta and his many reports and details of the harms its product was causing – not just to his son but to other children – went unresolved.

151. Meta designed its system in such a manner that it provided ambiguous, conflicting, and/or unpredictable responses, all of which were automated and generic. Meta did not provide any means or mechanism through which A.C. could interact directly with a human being capable of helping him address the serious and ongoing harms being caused to his child, and others.

152. On May 21, 2022, A.C. discovered that the Instagram predator was using another Instagram account. Not knowing whether Meta removed the reported account, A.C. had been regularly searching Instagram for the **_louis_moring_** username to make sure that the predatory account was not active. On May 21, when running this same search, a previously unidentified account that clearly belonged to the Instagram predator appeared.



The Instagram predator's username had gone from **_louis_moring_** to **louis_savoy_moring404** and even included the same photo as in the originally reported account.

153. On information and belief, the Instagram predator was also likely using the same IP address and device ID, which data Meta collects and tracks each time a user logs into their Instagram account. Some of this data is unique, such that Meta could easily enforce its terms and promises to users and parents and could protect users by simply not permitting banned users – like this Instagram predator – to access or open additional Instagram accounts. In fact, opening a new account after having one removed is explicitly in violation of Meta's terms of use. Yet, on information and belief, Meta does not take reasonable steps to identify banned users, as it would necessarily have to do in order to enforce its own terms.

154. Meta did not enforce its own terms in this instance, with regard to a violating user that A.C. was able to identify with a single key-word search. At the same time, Meta profits with each new account opened and used, and profited from its choice to allow the offending user to continue using its product.

155. But also, like this predatory user's prior account, this newly identified account already had hundreds of followers, which likely would mislead other minor users into thinking

that the account holder was who the account claimed they were – which A.C. does not believe to be the case. Either this account had been around for some time, or this account holder was able to utilize Meta's systems to quickly populate their account with followers.

156. However, Meta is able to quickly identify instances of abnormal and suspicious account activity, including things like follower churn and/or the addition of a significant number of followers from common sources, locations, and/or devices, which are indicative of predatory users and single user multiple accounts. Indeed, Meta claims to collect extensive and invasive personal, device, geographic, and other types of data for this very reason – to keep its users safe. Meta's Data Policy provides just some examples of the types of data it collects,

> • **Your usage.** We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.

While Meta's Data Policy and Terms of Use, respectively, claim that Meta is collecting this data in order to keep users safe and to investigate the types of reports Meta received from A.C.,

> **Promote safety, integrity and security.**
>
> We use the information we have to verify accounts and activity, combat harmful conduct, detect and prevent spam and other bad experiences, maintain the integrity of our Products, and promote safety and security on and off of Meta Products. For example, we use data we have to investigate suspicious activity or violations of our terms or policies, or to detect when someone needs help. To learn more, visit the Facebook Security Help Center and Instagram Security Tips.
>
> • **Fostering a positive, inclusive, and safe environment.**
> We develop and use tools and offer resources to our community members that help to make their experiences positive and inclusive, including when we think they might need help. We also have teams and systems that work to combat abuse and violations of our Terms and policies, as well as harmful and deceptive behavior. We use all the information we have-including your information-to try to keep our platform secure. We also may share information about misuse or harmful content with other Meta Companies or law enforcement. Learn more in the **Data Policy**.
>
> • **Developing and using technologies that help us consistently serve our growing community.**
> Organizing and analyzing information for our growing community is central to our Service. A big part of our Service is creating and using cutting-edge technologies that help us personalize, protect, and improve our Service on an incredibly large scale for a broad global community. Technologies like artificial intelligence and machine learning give us the power to apply complex processes across our Service. Automated technologies also help us ensure the functionality and integrity of our Service.

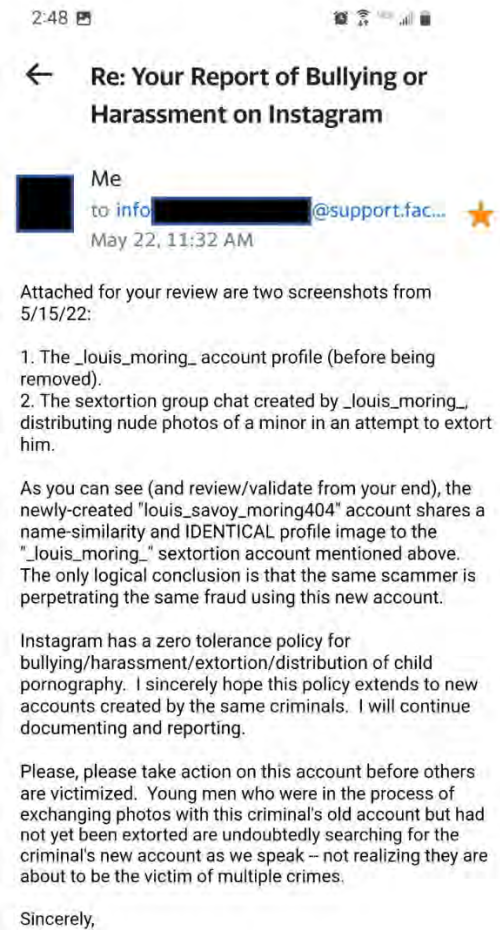
157. But as evidenced by what happened here, Meta does not in fact utilize the data it collects to keep its users safe – at least not in any reasonable and/or routine manner. If Meta did, it would be identifying and removing predators like this one well before they obtained hundreds, even thousands, of followers; and *before* they could exploit and abuse minor users, like John Doe, via Instagram and Meta's public profile and direct messaging product features.

158. Instead, this Instagram predator was able to open or access multiple accounts, even after being reported and despite Meta's actual knowledge that they were exploiting minors and knowingly circulating Child Sexual Abuse Material via Meta's Instagram product for purposes of extortion. Instagram had actual knowledge of the harms and victims of these abuses.

159. On May 21, A.C. immediately reported this additional Instagram account via the Instagram app and the "Report Violations of Our Community Guidelines" form on the Instagram website. A.C. provided the following details to Instagram via the web form,

> The louis_savoy_moring404 account is engaging in sextortion. Please see my ticket submitted on 5/17/22 regarding the _louis_moring_ user. This account is clearly a re-creation of the recently-removed "_louis_moring_" (identical profile picture, username/name similarity). The owner of these accounts is pretending to be a young woman; soliciting sexual images of men/boys (including minors/children); sharing the sexual images via Group Chat/Direct Message with the victim's friends, family, classmates, acquaintances/etc.; and threatening/demanding payment (extortion) for the removal of the images.
>
> As stated in this report and my previous report, the bullying/harassment/extortion/solicitation and distribution of child pornography is taking place in Group Chat/Direct Message, and I therefore am unable to report the content itself. My son is a victim of this crime, by this same individual/extortion group. I too feel personally violated and victimized by the malicious user's actions. I am extremely frustrated by Instagram's inability to identify/prevent this type of abuse -- especially in the case of a re-created account such a this, which is so easily identifiable and uses exactly the same profile image as the original.
>
> Lives are at risk every moment this account is left online (or any other accounts the owners create). Children are being bullied, extorted, harassed, and are at risk of suicide.
>
> I would like a representative of Instagram to follow up with me to confirm the removal of this account and detail how this ongoing criminal activity will be addressed moving forward.

On May 22, after seeing that the reported account was still active on Instagram, A.C. sent a detailed response to the automated email Meta's systems sent him,



2:48

Re: Your Report of Bullying or Harassment on Instagram

Me
to info[redacted]@support.fac...
May 22, 11:32 AM

Attached for your review are two screenshots from 5/15/22:

1. The _louis_moring_ account profile (before being removed).
2. The sextortion group chat created by _louis_moring_, distributing nude photos of a minor in an attempt to extort him.

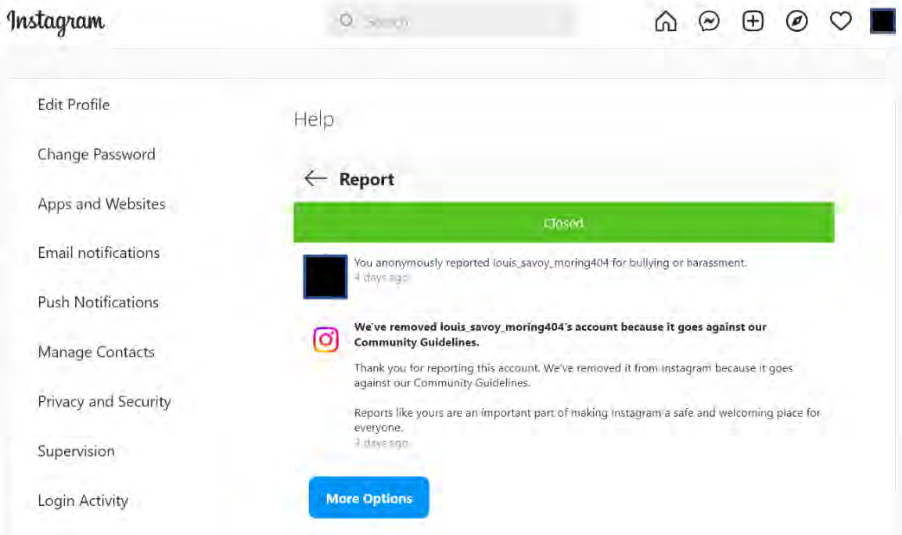
As you can see (and review/validate from your end), the newly-created "louis_savoy_moring404" account shares a name-similarity and IDENTICAL profile image to the "_louis_moring_" sextortion account mentioned above. The only logical conclusion is that the same scammer is perpetrating the same fraud using this new account.

Instagram has a zero tolerance policy for bullying/harassment/extortion/distribution of child pornography. I sincerely hope this policy extends to new accounts created by the same criminals. I will continue documenting and reporting.

Please, please take action on this account before others are victimized. Young men who were in the process of exchanging photos with this criminal's old account but had not yet been extorted are undoubtedly searching for the criminal's new account as we speak -- not realizing they are about to be the victim of multiple crimes.

Sincerely,

160. This time it didn't take Meta four days. A.C. received confirmation later on May 22 that the **louis_savoy_moring404** Instagram account had been removed for violating Instagram's Community Guidelines.



Instagram

Edit Profile
Change Password
Apps and Websites
Email notifications
Push Notifications
Manage Contacts
Privacy and Security
Supervision
Login Activity

Help

Report

Closed

You anonymously reported louis_savoy_moring404 for bullying or harassment.
4 days ago

We've removed louis_savoy_moring404's account because it goes against our Community Guidelines.

Thank you for reporting this account. We've removed it from Instagram because it goes against our Community Guidelines.

Reports like yours are an important part of making Instagram a safe and welcoming place for everyone.
4 days ago

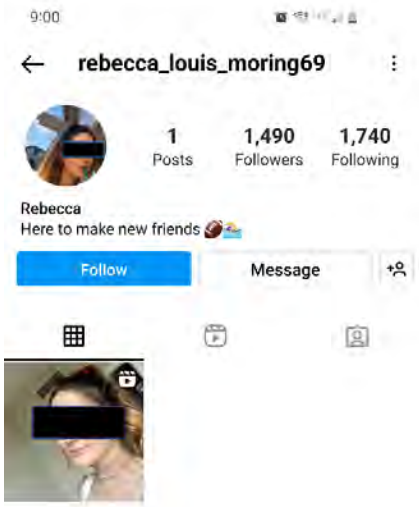
More Options

161. Only it turns out that Meta let the Instagram predator open a seemingly unlimited number of Instagram accounts, all using the same or similar photos and/or variations of the same first and last name. A.C. identified more than a dozen different accounts readily identifiable as belonging to this same Instagram predator. There are undoubtedly more; A.C. simply needed to stop looking for his own physical and emotional health.

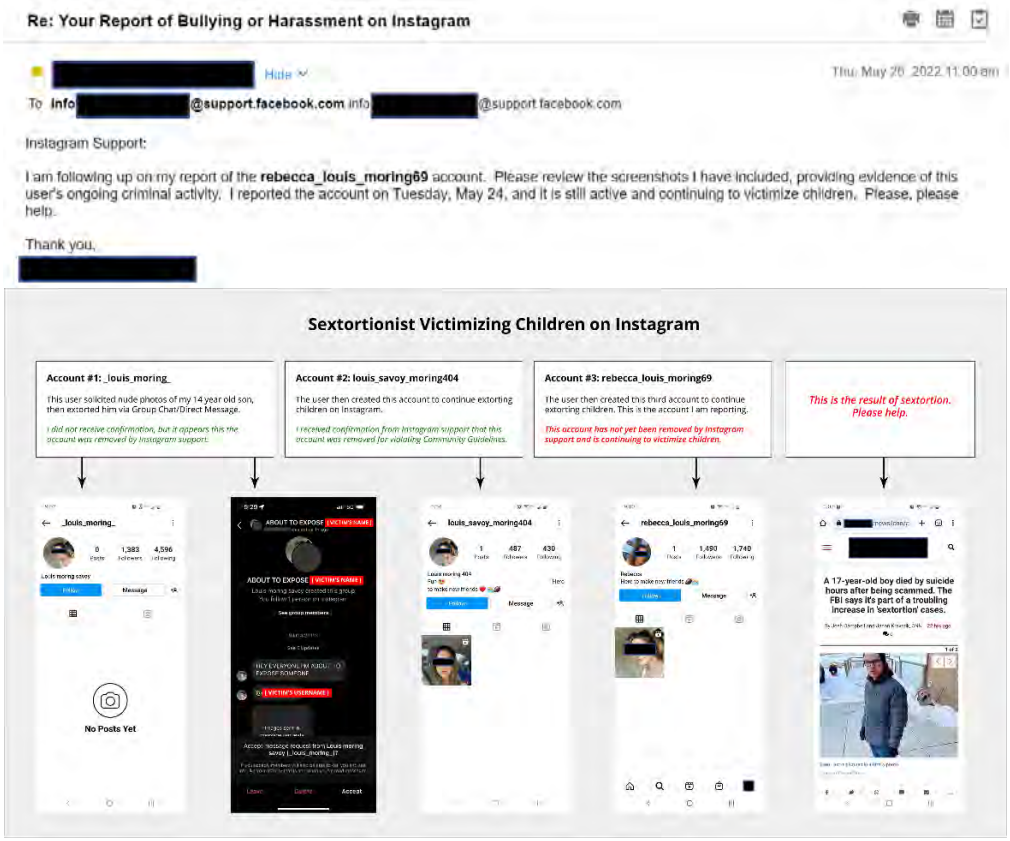
162. Meta could very easily use the data it collects to identify and block individuals who pose a threat to minors and have already been found to have violated Meta's terms in a serious and/or harmful manner. Meta has the ability to block not just the reported username, but all usernames reasonably associated with the violating user. This type of unilateral step would be taken without regard to any content and would protect millions of children from these types of harms; it would also, of course, impact Meta in that such predatory users would no longer be able to open and operate multiple Instagram accounts.

163. Meta does not warn minor users or their parents that it does not block users found to have violated its terms and/or used its product for illegal activities. On the contrary, Meta represents that it uses its technology and the data it collects from users to keep children safe.

164. On May 24, 2022, A.C. found another account opened by the Instagram predator, which embedded the same photo as the first two and used the same first and last name,



165. A.C. submitted the same types of reports, but this time Meta did nothing. On May 26, 2022, seeing that the **rebecca_louis_moring69** account was still active, A.C. sent a follow up email to Meta, including a graphic demonstrating the predator's account history, the ongoing situation, and the seriousness of the situation. He wrote, "Please review the screenshots I have included, providing evidence of this user's ongoing criminal activity. I reported the account on Tuesday, May 24, and it is still active and continuing to victimize children. Please, please help."



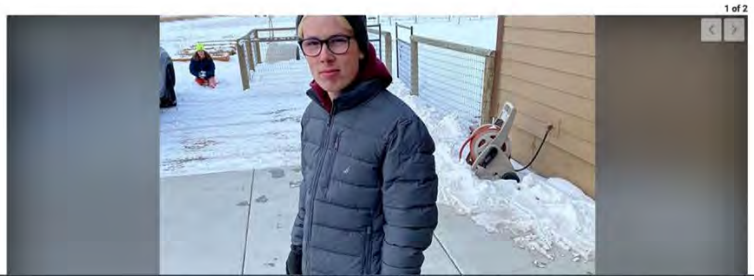
166. Only then did Meta remove the **rebecca_louis_moring69** account. It took multiple reports over several days and A.C. sending Meta a detailed timeline with screen shots, including an article about a 17-year-old boy who died of suicide after being sextorted.[8] A.C. wrote, "*This is the result of sextortion. Please help.*"

[8] https://www.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html

A 17-year-old boy died by suicide hours after being scammed. The FBI says it's part of a troubling increase in 'sextortion' cases.

By Josh Campbell and Jason Kravarik, CNN May 20, 2022 Updated Jun 26, 2022 0

1 of 2



Ryan Last received a message on a school night in February from someone he believed to be a girl.

Within hours, the 17-year-old, straight-A student and Boy Scout had died by suicide.

"Somebody reached out to him pretending to be a girl, and they started a conversation," his mother, Pauline Stuart, told CNN, fighting back tears as she described what happened to her son days after she and Ryan had finished visiting several colleges he was considering attending after graduating high school.

The online conversation quickly grew intimate, and then turned criminal.

The scammer -- posing as a young girl -- sent Ryan a nude photo and then asked Ryan to share an explicit image of himself in return. Immediately after Ryan shared an intimate photo of his own, the cybercriminal demanded $5,000, threatening to make the photo public and send it to Ryan's family and friends.

The San Jose, California, teen told the cybercriminal he could not pay the full amount, and the demand was ultimately lowered to a fraction of the original figure -- $150. But after paying the scammers from his college savings, Stuart said, "They kept demanding more and more and putting lots of continued pressure on him."

At the time, Stuart knew none of what her son was experiencing. She learned the details after law enforcement investigators reconstructed the events leading up to his death.

She had said goodnight to Ryan at 10 p.m., and described him as her usually happy son. By 2 a.m., he had been scammed, and taken his life. Ryan left behind a suicide note describing how embarrassed he was for himself and the family.

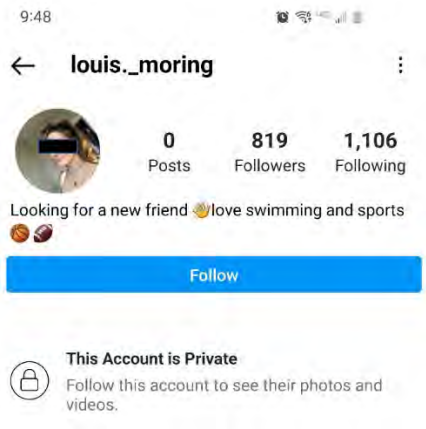
167. A.C. provided this information to Meta, in the hopes of reaching a human being at Meta who could help him protect his son and other children being harmed by the identified and

reported Instagram predator (in the exact same manner as described in this article). A.C. was terrified and shaken, thinking of how close his own son had come to these same feelings of despair because of what Snap and Meta did. A.C. felt an obligation to do everything he could to report this predator and to save other children from the same fate.

168. And at all times Meta had the ability to block the predatory user, but instead, its systems were designed in such a manner that A.C. had no way to connect with a living person; and when he did manage to get a report submitted through Meta's defective in-app and Help Center reporting mechanisms, Meta's responses were inconsistent and unhelpful.

169. Meta at all times had the ability to block predatory users on a unilateral basis but delayed and/or failed to do so. More children were victimized as a direct and proximate result.

170. To this day, the Instagram predator continues to operate on the Instagram platform without consequence and Meta continues to profit directly and/or indirectly as a result. A.C. has identified numerous different accounts, which identification is quick and easy – even without the knowledge and resources of Meta Platforms, Inc. The following is just one more example, which account A.C. identified on June 13, 2022,

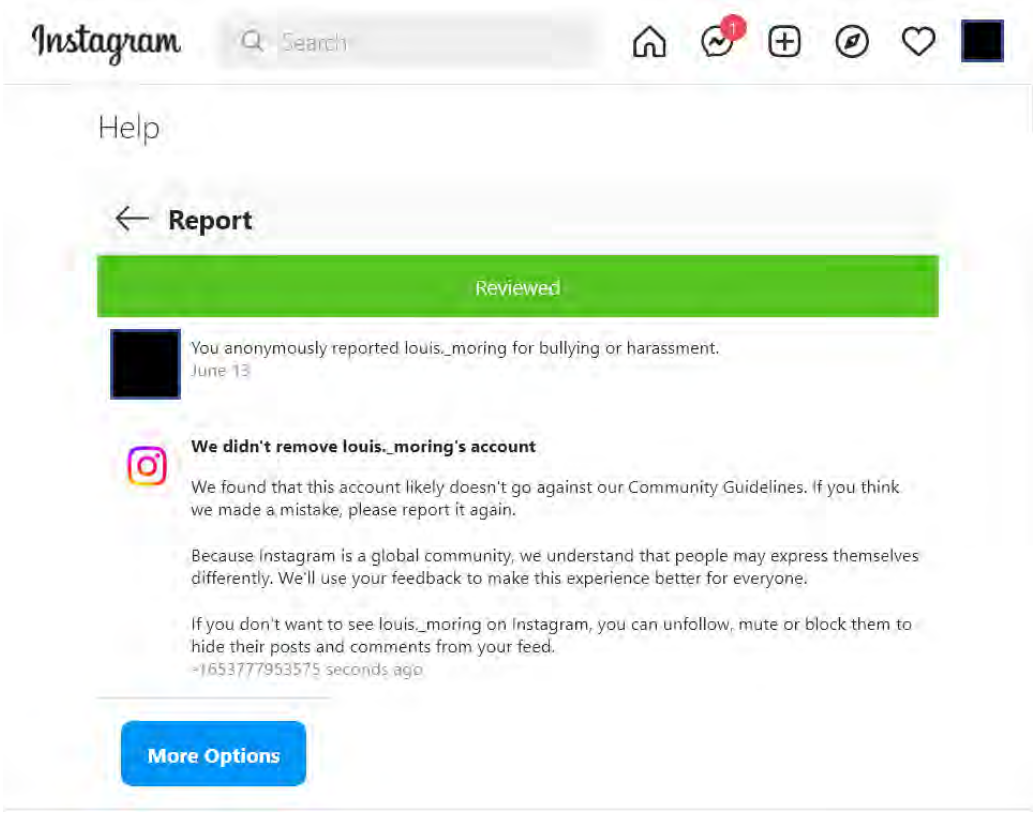


171. Again, the Instagram predator used the *same* photo and *same* first and last name as part of their Instagram Username. Again, A.C. reported the Instagram predator to Meta, using the *same* methods he used to report the other violating accounts.

//

172. This time, however, Meta sent A.C. two entirely different automated responses, depending on whether he accessed Instagram via his web browser or the app. Both responses stated that Meta had not or would not be acting on A.C.'s report.

173. Specifically, when A.C. checked with the web browser, Meta's automated response was that the account "likely doesn't go against [Meta's] Community Guidelines."



174. Though when A.C. checked in-app, Meta's response to the same report once again differed. In-app, Meta told A.C. that it didn't remove the account due to the high volume of reports Meta receives. That is, three days later and according to Meta's in-app message it had not yet even reviewed the report of exploitation and abuse.

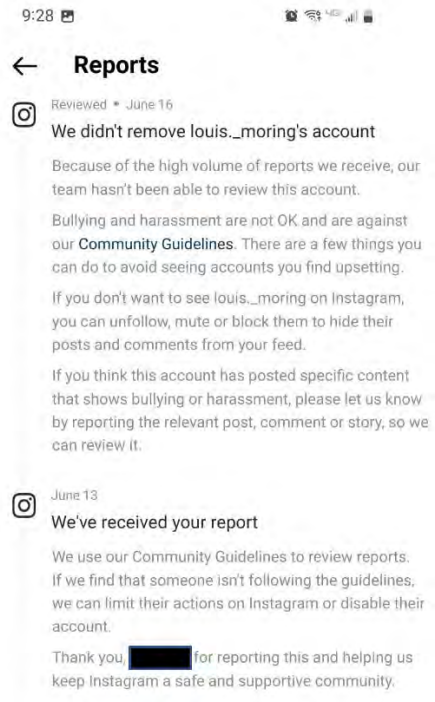
//

//

//

//

//



175. Following the above responses from Meta, A.C. submitted additional reports and documentation to Meta in further hopes that Meta would act. As of June 23, 2022 – 10 days after discovering the account and submitting the initial report – the **louis._moring** account was still active on the Instagram platform.

176. This user also and again has a significant number of followers, particularly if the account was relatively new – suggesting a common pattern, which would also be identifiable and known to Meta itself, but to no one else. Meta has the ability to cross reference the multiple reported accounts, check their followers and the time and manner in which those followers were added, and enforce the law and its own terms by using that data to identify and stop known Instagram predators actively using the Instagram product to prey on minor users.

177. Meta was negligent, if not willful, in its failure to remove accounts operated by this particular Instagram predator despite A.C.'s continued reporting and submission of ever-growing details and evidence.

178. At this point, A.C. is trying to protect not just his minor child but the other minors who are being exploited and abused because of Meta's Instagram product, while Meta itself

continues to profit directly and indirectly from this criminal enterprise. Indeed, the above photos are just *some* of the reports and information A.C. provided to Meta in and after May 2022.

179. In June of 2022, John Doe began complaining of various problems, including headaches, inability to sleep and waking up with racing thoughts, rapid heartbeat, sharp, localized pain that comes and goes in his neck, lower back, and legs, tingling and numbness in his palms and fingertips, shortness of breath and feeling like he "can't breathe or take a deep breath," jaw clenching, mood fluctuations, and stress and anxiety.

180. John Doe reported in the weeks that followed that what happened in May 2022 popped into his head a couple times each day. He tried to not think about it, but then it would be there, and he felt inside like he did when the whole thing happened. He felt like his world was falling apart; he suffered from a generalized feeling of doom, which he couldn't shake the rest of the day.

181. A.C. has taken John Doe to the doctor and is taking him to counseling. John Doe has been seriously and irreparably harmed. He has worked on these issues for several months with professional support and the ongoing support of his family; and the current plan is to take things day-by-day and see how they progress.

182. A.C. has also been seriously and irreparably harmed as a result of Meta's distribution of its social media product to his son, its complete failure to provide any reasonable reporting mechanism in connection with that distribution, and its failure to act despite A.C.'s many detailed reports and pleas for help.

183. A.C.'s mental and physical health have suffered greatly as a direct and proximate result of Instagram's actions and failures to act. A.C. cannot sleep or stay asleep most nights and wakes up in a panic. He has not had a good night's sleep for months and cannot stop thinking about the harms to his son and the harms Meta is causing other children, up to and including exploitation and even suicide.

184. A.C. is suffering extreme anxiety and stress as a direct and proximate result of Meta's actions and failure to act to the point where it is impacting every aspect of his life and

health. He can no longer work for more than small periods of time, which has severely impacted his income and livelihood. He is having vision problems due to the stress, as well as incredible physical pain, including but not limited to extreme abdominal pain, trouble breathing, neck, shoulder, and back pain, and multiple other physical symptoms that have made it difficult for A.C. to perform basic functions on a day-to-day basis.

185. A.C. is struggling with his mental and physical health far beyond anything he has ever experienced, to the point where it feels like something is broken inside of him. He cannot stop thinking and worrying about his son and the kids Meta is actively harming by allowing this known Instagram Predator to continue using its social media product for exploitation and abuse. He worries to the point of paralysis about the kids suffering the same trauma and life-altering harms foisted on his son and, even more, the kids who will turn to suicide as a result. For the first time in his life, A.C. feels as though things are out of control. He is struggling under the knowledge that there is literally nothing more he can do to help those children, due to the way Meta decided to design and operate its product, and yet he feels as though he cannot move forward unless he tries to help to them.

186. A.C. is struggling with the pain and guilt of knowing what is taking place on Instagram, the children who are being harmed, and how Meta could stop these harms; then having to live with the reality that he is doing everything he can and that despite all of his technical knowledge, experience, and efforts to get help, he cannot make Meta act. Despite this realization, A.C. feels a moral obligation to do more and is drowning under the guilt of not being able to protect children from harm.

187. But for Defendants' failure to conduct reasonable verification of age, identity, and/or parental consent, John Doe would not have been exposed to Instagram and Snap's inherently addictive and dangerous social media products and product features.

188. But for Defendants' targeted marketing, misleading representations, and inherently defective and/or harmful disappearing message products, John Doe would not have suffered the exploitation and harms he did.

189. But for Defendant Meta's inherently defective product, failure to provide effectual reporting mechanisms, and failure to act despite actual knowledge of harmful, illegal, and/or violating conduct perpetrated on minors because of its Instagram product, John Doe would not have suffered the exploitation and harms herein, and A.C. would not be suffering the ongoing mental anguish and emotional distress caused by his inability to protect his son and other children.

190. A.C. is a web developer and considers himself sophisticated when it comes to computers, systems, and technology in general. He took all reasonable and recommended steps to protect and watch over his son, and to monitor his son's online activities, and then took every step available to prevent and mitigate the harms the moment he learned of them. Yet still, his knowledge and expertise never stood a chance against Meta's drive to increase engagement at any cost.

VI. PLAINTIFF'S CLAIMS

COUNT I - STRICT PRODUCT LIABILITY (Design Defect)

191. Plaintiffs reallege each of the allegations in the preceding paragraphs as if full set forth herein.

192. Under Restatement (Second) of Torts § 402(a) and California law, one who sells any product in a defective condition unreasonably dangerous to the user is subject to liability for physical harm thereby caused to the user if (a) the seller is engaged in the business of selling such a product, and (b) it is expected to and does reach the user or consumer without substantial change in the condition which it was sold.

193. Defendants' products are defective because the foreseeable risks of harm posed by the product's design could have been reduced or avoided by the adoption of a reasonable alternative design by Defendants and the omission of the alternative design renders the product not reasonably safe. These defective conditions rendered these products unreasonably dangerous to persons or property and existed at the time the product left Defendants' control, reached the user or consumer without substantial change in the condition, and its defective condition was a cause of Plaintiff's injury.

194. Defendants designed, manufactured, marketed, and sold social media products that were unreasonably dangerous because they were designed to be addictive to the minor users to whom Defendants actively marketed and because the foreseeable use of Defendants' products causes mental and physical harm to minor users.

195. Defendants' products were unreasonably dangerous because they contained numerous design characteristics that are not necessary for the utility provided to the user but are unreasonably dangerous and implemented by Defendants solely to increase the profits they derived from each additional user and the length of time they could keep each user dependent on their product.

196. Defendants' products were unreasonably dangerous because they contain no effectual reporting mechanisms, or other means to ensure user safety, despite the incredible and inherent dangers they pose to minor users.

A. Inadequate Safeguards From Harmful and Exploitative Content

197. Snapchat and Instagram are defectively designed.

198. As designed Snapchat and Instagram's recommendation and other product features are not reasonably safe because they affirmatively direct minor users to harmful and exploitative content while failing to deploy feasible safeguards to protect vulnerable teens from such harmful exposures. It is feasible to design an algorithm and technologies that do not direct minors to harmful content by design, and to do so without altering, modifying, or deleting any third-party content posted on Defendants' social media products. The cost of designing these products to incorporate such safeguards would be negligible while benefit would be high in terms of reducing the quantum of mental and physical harm sustained by minor users and their families.

199. As designed, Snapchat and Instagram recommendations and other product features are not reasonably safe because they affirmatively direct and recommend minor users to harmful groups and other users, while failing to deploy feasible safeguards to protect vulnerable teens from such harmful exposures. It is feasible to design an algorithm and technologies that do not make harmful connection recommendations to minor users, or any connection recommendations at all;

it is feasible to design an algorithm and technologies that do not recommend harmful groups to minor users, or any group recommendations at all; and it is feasible to restrict access to minor users by strangers and adult users via direct messaging, to restrict and limit such access to users already on a minor user's "friend" list, or to prevent such access altogether. Defendants know that these product features cause a significant number of harms to their minor users, such as sexual exploitation, bullying, and encouragement of self-harm and suicide.

200. Reasonable users (and their parents) would not expect that Defendants' products would knowingly expose them to such risks and dangers and/or that Defendants' products would direct them to harmful users at all, much less in the manipulative and coercive manner that they do. Defendants have and continue to knowingly use their algorithms and other technologies on users in a manner designed to affirmatively change their behavior, which methods are particularly effective on (and harmful to) Defendants' youngest users.

B. Failure to Verify Minor Users' Age and Identity

201. Snapchat and Instagram are defectively designed.

202. As designed, Defendants' products are not reasonably safe because they do not provide for adequate age verification by requiring users to document and verify their age and identity.

203. Adults frequently set up user accounts on Defendants' social media products disguising their identity and/or posing as minors to groom unsuspecting minors to exchange sexually explicit content and images, which frequently progresses to sexual exploitation and trafficking, and commercial sex acts.

204. Minor users of social media and their parents do not reasonably expect that prurient adults set up fraudulent accounts on Defendants' social media products and pose as minors for malign purposes. Moreover, and as Defendants know, minor users lack the life experience and frontal lobe development necessary to protect themselves from such predators – providing access to these children is an inherently dangerous product mechanic, which dangers are known and have been studied by these defendants but were not otherwise known to the general public.

205. Minor users whose parents have taken affirmative steps to keep them away from Defendants' products often open multiple accounts, such that Defendants know or have reason to know that the user is underage and/or does not have parental permission to use their product. Defendants already have the information and means they need to ascertain with reasonable certainty their users' actual age. Defendants utilize these tools to investigate, assess, and report on percentages and totals of underage users for internal assessment purposes. They then choose to simply do nothing about that information as it relates to the specific, underaged users themselves.

206. But also, predator users who are engaged in illegal, harmful, and/or violating activities also often open multiple accounts, such that Defendants know or have reason to know that the user is engaged in such harmful conduct and/or has violated their terms such that their use of the product is no longer duly authorized. Defendants are encouraging and creating these dangers and enabling these predators through their product features and refusal to enforce their own terms. Defendants also already have the information and means they need to ascertain with reasonable certainty their users' actual age, and when one user has multiple accounts. Defendants utilize these tools to investigate, assess, and report on percentages and totals of underage users for internal assessment purposes. They then choose to simply do nothing about that information as it relates to the specific, predatory users themselves, to the detriment of other, vulnerable users – including kids, to whom Defendants market and addictively design their products.

207. Reasonably accurate age and identity verification is not only feasible but widely deployed by online retailers and internet service providers. Defendants not only can estimate the age of their users, but they do.

208. The cost of incorporating age and identify verification into Defendants' products would be negligible, whereas the benefit of age and identity verification would be a substantial reduction in severe mental health harms, sexual exploitation, and abuse among minor users of Defendants' products and would discourage the use of said products for exploitation and abuse of minors.

C. Provision of Inadequate and Unreasonable Parental Control and Monitoring Products and Processes

209. Snapchat and Instagram are defectively designed.

210. Defendants have intentionally designed products to frustrate the exercise of parental responsibility by their minor users' parents. Parents have a right to monitor their children's social media activity to protect them from harm. Defendants have designed products that make it difficult, if not impossible, for parents to exercise parental responsibility.

211. It is feasible to design a social media product that requires parental consent for users under the age of 18 and prohibits users under the age of 13.

212. Defendants' products are also defective for lack of parental controls, permission, and monitoring capability available on many other devices and applications.

213. Defendants' products are designed with specific product features intended to prevent and/or interfere with parents' reasonable and lawful exercise of parental control, permission, and monitoring capability available on many other devices and applications.

D. Design of Addictive Social Media Products

214. Snapchat and Instagram are defectively designed.

215. As designed, Defendants' social media products are addictive to minor users as follows: When minors use design features such as "likes" it causes their brains to release dopamine, which creates short term euphoria. However, as soon as dopamine is released, minor users' brains adapt by reducing or "downregulating" the number of dopamine receptors that are stimulated and their euphoria is countered by dejection. In normal stimulatory environments, this dejection abates, and neutrality is restored. However, Defendants' algorithms are designed to exploit users' natural tendency to counteract dejection by going back to the source of pleasure for another dose of euphoria. As this pattern continues over a period of months and the neurological baseline to trigger minor users' dopamine responses increases, they continue to use the social media products at issue, not for enjoyment, but simply to feel normal. Once they stop using these products, minor users experience the universal symptoms of withdrawal from an addictive substance including

anxiety, irritability, insomnia, and craving.

216. Addiction is not restricted to substance abuse disorders. Rather, the working definition of addiction promulgated in the seminal article *Addictive behaviors: Etiology and Treatment* published by the American Psychological Association in its 1988 *Annual Review of Psychology* defines addiction as,

> a repetitive habit pattern that increases the risk of disease and/or associate personal and social problems. Addictive behaviors are often experienced subjectively as 'loss of control' – the behavior contrives to occur despite volitional attempts to abstain or moderate use. These habit patterns are typically characterized by immediate gratification (short term reward), often coupled with delayed deleterious effects (long term costs). Attempts to change an addictive behavior (via treatment or self-initiation) are typically marked with high relapse rate.

217. Addiction researchers agree that addiction involves six core components: (1) salience—the activity dominates thinking and behavior; (2) mood modification—the activity modifies/improves mood; (3) tolerance—increasing amounts of the activity are required to achieve previous effects; (4) withdrawal—the occurrence of unpleasant feelings when the activity is discontinued or suddenly reduced; (5) conflict—the activity causes conflicts in relationships, in work/education, and other activities; and (6) relapse—a tendency to revert to earlier patterns of the activity after abstinence or control.

218. Social media addiction has emerged as a problem of global concern, with researchers all over the world conducting studies to evaluate how pervasive the problem is. Addictive social media use is manifested when a user (1) becomes preoccupied by social media (salience); (2) uses social media in order to reduce negative feelings (mood modification); (3) gradually uses social media more and more in order to get the same pleasure from it (tolerance/craving); (4) suffers distress if prohibited from using social media (withdrawal); (5) sacrifices other obligations and/ or causes harm to other important life areas because of their social media use (conflict/functional impairment); and (6) seeks to curtail their use of social media without success (relapse/loss of control).

219. The Bergen Facebook Addiction Scale (BFAS) was specifically developed by psychologists in order to assess subjects' social media use using the aforementioned addiction

criteria, and is by far the most widely used measure of social media addiction. Originally designed for Facebook, BFAS has since been generalized to all social media. BFAS has been translated into dozens of languages, including Chinese, and is used by researchers throughout the world to measure social media addiction.

220. BFAS asks subjects to consider their social media usage with respect to the six following statements and answer either (1) very rarely, (2) rarely, (3) sometimes, (4) often, or (5) very often,

a. You spend a lot of time thinking about social media or planning how to use it.

b. You feel an urge to use social media more and more.

c. You use social media in order to forget about personal problems.

d. You have tried to cut down on the use of social media without success.

e. You become restless or troubled if you are prohibited from using social media.

f. You use social media so much that it has had a negative impact on your job/studies.

Subjects who score a "4" or "5" on at least 4 of those statements are deemed to suffer from social media addiction.

221. Addictive use of social media by minors is psychologically and neurologically analogous to addiction to internet gaming disorder as described in the American Psychiatric Association's 2013 Diagnostic and Statistical Manual of Mental Disorders (DSM-5), which is used by mental health professionals to diagnose mental disorders. Gaming addiction is a recognized mental health disorder by the World Health Organization and International Classification of Diseases and is functionally and psychologically equivalent to social media addiction. The diagnostic symptoms of social media addiction among minors are the same as the symptoms of addictive gaming promulgated in DSM-5 and include:

a. Preoccupation with social media and withdrawal symptoms (sadness, anxiety, irritability) when device is taken away or not possible (sadness,

anxiety, irritability).

b. Tolerance, the need to spend more time using social media to satisfy the urge.

c. Inability to reduce social media usages, unsuccessful attempts to quit using social media.

d. Giving up other activities, loss of interest in previously enjoyed activities due to social media usage.

e. Continuing to use social media despite problems.

f. Deceiving family members or others about the amount of time spent on social media.

g. The use of social media to relieve negative moods, such as guilt or hopelessness.

h. and Jeopardized school or work performance or relationships due to social media usage.

222. Defendants' advertising profits are directly tied to the quantity of their users' online time and engagement, and their algorithms and other product features are designed to maximize the time users spend using the product by directing them to content that is progressively more and more stimulative. Defendants enhance advertising revenue by maximizing users' time online through a product design that addicts them to the platform.

223. It is feasible to make Defendants' products not addictive to minor users by turning off the algorithms, limiting the frequency and duration of access, and suspending service during sleeping hours. Designing software that limits the frequency and duration of minor users' screen use and suspends service during sleeping hours could be accomplished at negligible cost; whereas the benefit of minor users maintaining healthy sleep patterns would be a significant reduction in depression, attempted and completed suicide, and other forms self-harm among this vulnerable age cohort.

//

E. Inadequate Notification of Parents of Dangerous and Problematic Social Media Usage by Minor Users

224. Snapchat and Instagram are defectively designed.

225. Defendants' products are not reasonably safe as designed because they do not include any safeguards to notify users and their parents of usage that Defendants knows to be problematic and likely to cause negative mental health effects to users, including excessive passive use and use disruptive of normal sleep patterns. This design is defective and unreasonable.

226. It is reasonable for parents to expect that social media products that actively promote their platform to minors will undertake reasonable efforts to notify parents when their child's use becomes excessive. It is feasible for Snapchat and Instagram to design a product that identifies a significant percentage of their minor users who are using the product more than three hours per day or using it during sleeping hours at negligible cost.

227. Likewise, it is feasible for Snapchat and Instagram to design a product that notifies parents when strangers attempt to engage directly with them, and/or otherwise limits the ability to find and access minors on their platforms, absent parental consent.

228. Defendants' products are not reasonably safe as designed because, despite numerous reported instances of child sexual solicitation and exploitation by adult users, Defendants have not undertaken reasonable design changes to protect underage users from this abuse, including notifying parents of underage users when they have been messaged or solicited by an adult user or when a user has sent inappropriate content to minor users or even blocking users known to be engaged in exploitation and abuse because of their products.

229. Defendants' entire business is premised upon collecting and analyzing user data and it is feasible to use Defendants' data and algorithms and other technologies to identify and restrict improper sexual solicitation, exploitation, and abuse by adult users.

230. Moreover, it is reasonable for parents to expect that platforms such as Instagram and Snapchat, which actively promote their services to minors, will undertake reasonable efforts to identify users suffering from mental injury, self-harm, or sexual abuse and implement

technological safeguards to notify parents by text, email, or other reasonable means that their child is in danger; and to identify abusive and violating users and block them.

231. As a proximate result of these dangerous and defective design attributes of Defendants' products, John Doe suffered severe mental harm. Plaintiffs did not know, and in the exercise of reasonable diligence could not have known, of these defective design attributes in Defendants' products prior to 2022.

232. As a result of these dangerous and defective design attributes of Defendants' products, Plaintiff A.C. suffered emotional distress, physical harms, and pecuniary hardship arising from both his son's mental harm and Defendant Meta's refusal to accept and act on his well-documented reports.

233. Defendants are further liable to Plaintiffs for punitive damages based upon the willful and wanton design of their products that were intentionally marketed and sold to underage users, whom they knew would be seriously harmed through their use of Snapchat and Instagram.

COUNT II – STRICT PRODUCT LIABILITY (Failure to Warn)

234. Plaintiffs reallege each of the allegations in the preceding paragraphs as if full set forth herein.

235. Defendants' products are defective because of inadequate instructions or warnings because the foreseeable risks of harm posed by these products could have been reduced or avoided by the provision of reasonable instructions or warnings by the manufacturer and the omission of the instructions or warnings renders the product not reasonably safe. This defective condition rendered the products unreasonably dangerous to persons or property, existed at the time the products left Defendants' control, reached the user or consumer without substantial change in the condition in which they were sold, and were a cause of Plaintiff's injuries.

236. Defendants' products are unreasonably dangerous and defective because they contain no warning to users or parents regarding the addictive design and effects and inherent defects of Instagram and Snapchat.

//

237. Defendants' social media product rely on highly complex and proprietary algorithms and similar technologies that are both undisclosed and unfathomable to ordinary consumers, who do not expect that social media platforms are physically and/or psychologically addictive.

238. The magnitude of harm from use of Defendants' products is horrific, ranging from simple diversion from academic, athletic, and face-to-face socialization to sleep loss, severe depression, anxiety, self-harm, and suicide.

239. The harms resulting from minors' addictive use of social media platforms have been not only well-documented in professional and scientific literature, but Defendants had actual knowledge of such harms.

240. Defendants' products are unreasonably dangerous because they lack any warnings that foreseeable product use can disrupt healthy sleep patterns or specific warnings to parents when their child's product usage exceeds healthy levels or occurs during sleep hours. Excessive screen time is harmful to adolescents' mental health and sleep patterns and emotional well-being. Reasonable and responsible parents are not able to accurately monitor their child's screen time because most adolescents own or can obtain access to mobile devices and engage in social media use outside their parents' presence.

241. It is feasible for Defendants' products to report the frequency and duration of their minor users' screen time to their parents without disclosing the content of communications at negligible cost.

242. It is feasible for Defendants' products to report dangerous and/or harmful events impacting minor users to minor users' parents at negligible cost.

243. Defendants knew about these harms, knew that users and parents would not be able to safely use their products without warnings, and failed to provide warnings that were adequate to make the product reasonably safe during ordinary and foreseeable use by children.

244. As a result of Defendants' failure to warn, John Doe suffered mental harm from his use of Instagram and Snapchat.

245. As a result of Defendants' failure to warn, Plaintiff A.C. has suffered emotional distress, physical harm, and pecuniary hardship.

246. Defendants are further liable to Plaintiffs for punitive damages based upon their willful and wanton failure to warn of known dangers of their products that were intentionally marketed and sold to teenage users, whom they knew would be seriously harmed through their use of Instagram and Snapchat.

COUNT III – NEGLIGENCE

247. Plaintiffs reallege each of the allegations in the preceding paragraphs as if full set forth herein.

248. At all relevant times, Defendants had a duty to exercise reasonable care and caution for the safety of individuals using their products, such as John Doe

249. Defendants owe a heightened duty of care to minor users of their social media products because adolescents' brains are not fully developed, resulting in a diminished capacity to make good decisions regarding social media usage, eschew self-destructive behaviors, and overcome emotional and psychological harm.

250. As product manufacturers marketing and selling products to consumers, Defendants owed a duty to exercise ordinary care in the manufacture, marketing, and distribution of their products, including a duty to warn minor users and their parents of hazards that Defendants knew to be present, but not obvious, to underage users and their parents.

251. As business owners, Defendants owe their users who visit their social media platforms and from whom they derive billions of dollars per year in revenue a duty of ordinary care substantially similar to that owed by physical business owners to its business invitees.

252. Defendants were negligent, grossly negligent, reckless and/or careless in that they failed to exercise ordinary care and caution for the safety of underage users, like John Doe, using their social media products.

253. Defendants were negligent in failing to conduct adequate testing and failing to allow independent academic researchers to adequately study the effects of their products and levels

of problematic use amongst teenage users. Defendants know that their products are harmful, cause extensive mental harm, and that minor users are engaging in problematic and addictive use that their parents are helpless to monitor and prevent.

254. Defendants were negligent in failing to provide adequate warnings about the dangers associated with the use of social media products and in failing to advise users and their parents about how and when to safely use their social media platforms and features.

255. Defendants were negligent in failing to fully assess, investigate, and restrict the use of their social media products by adults to sexually solicit, abuse, manipulate, and exploit minor users of their social media products.

256. Defendants were negligent in failing to provide users and parents the tools to ensure their social media products are used in a limited and safe manner by underage users.

257. Defendants were negligent in failing to provide users and parents with reasonable and effectual reporting mechanisms, and for failing to enforce their own terms of service upon notice of illegal conduct and/or violations of terms – which failures resulted in harm to other users, including minor users who should not have had access to Defendants' products in the first place.

258. As a result of Defendants' negligence, John Doe suffered severe mental harm.

259. As a result of Defendants' negligence, Plaintiff A.C. suffered emotional distress, physical harm, and pecuniary hardship.

260. Defendants are further liable to Plaintiffs for punitive damages based upon their willful and wanton conduct toward underage users, including John Doe, whom they knew would be seriously harmed through the use of their social media products.

COUNT IV – VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, CAL. BUS & PROF. CODE §§ 17200, et seq.

261. Plaintiffs reallege each of the allegations in the preceding paragraphs as if full set forth herein.

262. Defendants are corporations and thus each of them is a "person," as defined by California Business & Professions Code § 17201.

263. The UCL prohibits all conduct that is unlawful, unfair, or fraudulent.

264. Defendants' conduct is unlawful as set forth in Counts I–III, above.

265. Defendants' conduct is unlawful because they have knowledge of users under the age of 18 on their platforms who lack parental consent to use their products and, in fact, actively target, market to, and encourage use of their social media products by minors under the age of 18 who lack parental consent to use their products.

266. Defendants engaged in fraudulent and deceptive business practices in violation of the UCL by promoting products to underage users, including John Doe, while concealing critical information regarding the addictive nature and risk of harm these products pose. Defendants knew and should have known that their statements and omissions regarding the addictive and harmful nature of their products were misleading and therefore likely to deceive the members of the public who use Defendants' products and who permit their underage children to use Defendants' products. Had Plaintiffs known of the dangerous nature of Defendants' products, he would have taken early and aggressive steps to stop or limit his son's use of them.

267. Defendants' practices are unfair and violate the UCL because they offend established public policy, and because the harm these practices cause to consumers greatly outweighs any benefits associated with them. Additionally, Defendants have designed their products to lock-in users, especially children and teens. They know that minors want to use their products and that the more minors invest in Defendants' products the harder it is for them to switch. It is hard to switch because of network effects and sunk costs, and Defendants design their products explicitly around these designs for the purpose of locking-in users. As of now, each of these defendants have locked-in the majority (possibly over 80%) of all U.S. teens aged 13 to 17 and with access to the internet. Defendants are actively working to hit 100%.

268. Defendants' conduct has resulted in substantial injuries that Plaintiffs could not reasonably have avoided because of Defendants' deceptive conduct. This substantial harm is not outweighed by any countervailing benefits to consumers or competition.

//

269. As a direct and proximate result of the foregoing acts and practices, Defendants have received, or will receive, income, profits, and other benefits, which they would not have received if they had not engaged in the violations of the UCL described herein. As a direct and proximate result of the foregoing acts and practices, Defendants have also obtained unfair advantages over similar businesses that have not engaged in such practices.

270. As a result of Defendants' UCL violations, Plaintiffs have suffered injury in fact and lost money as set forth herein.

271. Accordingly, Plaintiffs seek injunctive and equitable relief to halt and remedy Defendant's unlawful, fraudulent, and unfair conduct.

COUNT V – UNJUST ENRICHMENT

272. Plaintiffs reallege each of the allegations in the preceding paragraphs as if full set forth herein.

273. As a result of Defendants' conduct detailed herein, Defendants received a benefit. Because Defendants' advertising profits are directly tied to the number of user accounts and the amount of time those users spend on Instagram, Defendants benefited directly from John Doe's unauthorized use of their products and also from the predatory user (and predatory users in general) enabled and assisted by Defendants' products.

274. It would be unjust and inequitable for Defendants to retain the ill-gotten benefits at Plaintiff's expense, in light of Defendants' acts and omissions described herein.

275. Accordingly, Plaintiffs seek damages in an amount to be proven at trial.

COUNT VI – INVASION OF PRIVACY

(California Constitutional Right to Privacy, Cal. Const. Art. 1, § 1)

276. Plaintiffs reallege each of the allegations in the preceding paragraphs as if full set forth herein.

277. Defendants intentionally intruded upon Plaintiff's solitude, seclusion, or private affairs by designing their product with features that frustrate and interfere with parents' ability to monitor and control their children's social media usage.

278. These intrusions are highly offensive to a reasonable person, particularly given Defendants' interference with the fundamental right of parenting and their exploitation of children's special vulnerabilities for commercial gain.

279. Plaintiffs were harmed by Defendants' invasion of privacy, as detailed herein.

280. Plaintiffs therefore seek compensatory and punitive damages in amounts to be determined at trial, as well as injunctive relief requiring Defendants to cease the harmful practices described throughout this complaint.

COUNT VII – INFLICTION OF EMOTIONAL DISTRESS

(as against Defendant Meta only)

281. Plaintiffs reallege each of the allegations in the preceding paragraphs as if full set forth herein.

282. Defendant Meta engaged in extreme and outrageous conduct with reckless disregard of the probability of causing severe emotional distress to Plaintiffs and others when it failed to provide parents with a reasonable and effective means to report unauthorized use, illegal conduct, and violations of Meta's terms of service that posed significant danger to their children and other young users.

283. Defendant Meta likewise engaged in extreme and outrageous conduct when it received notice of the publication of CSAM from a concerned parent and failed to respond, delayed its response, and/or ultimately failed to act reasonably to protect its minor users.

284. Defendant Meta likewise engaged in extreme and outrageous conduct when it made the decision to allow the Instagram predator to continue using its product, and ignored repeated reports, with documentation, and pleas from Plaintiff A.C. to protect its minor users.

285. A.C. first reported the predator account on May 14 and reported it from both John Doe's Instagram as well as his own. Meta proceeded to not respond and delay its response, then claimed technical issues. It took several days for the user account to go dark, but even then, Meta refused to say whether it had disabled the account and/or whether any action had been taken with the Group Chat created to sextort A.C.'s minor child – in fact, Meta was instead allowing the

Group Chat to continue, with addition of more users and escalating publication of CSAM, despite actual knowledge of what had occurred.

286. Meta's own internal documents make clear that it is aware of the dangers of its product, including the potential for exploitation and abuse. Despite this knowledge, Meta has refused to provide parents with any reasonable and effective means to report such harms and protect their children.

287. Meta's conduct was outrageous and offensive by any measure.

288. It is inconceivable that any company would distribute its product to children and then fail to provide parents with a means to contact them and/or effectively report harms once discovered – though that is precisely what Meta did.

289. Plaintiff A.C. has suffered severe emotional, physical, and pecuniary harms as a result.

290. Plaintiffs therefore seek damages in amounts to be determined at trial.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment against Meta and Snap for monetary damages for the following harms:

1. Past and ongoing physical and mental pain and suffering of John Doe, in an amount to be more readily ascertained at the time and place set for trial.

2. Loss of future income and earning capacity of John Doe

3. Past and future medical expenses of John Doe

4. Monetary damages suffered by A.C.

5. Loss of future income and earning capacity of A.C.

6. Past and future medical expenses of A.C.

7. Past and ongoing physical and mental pain and suffering of A.C., in an amount to be more readily ascertained at the time and place set for trial.

8. Punitive damages.

9. For the reasonable costs and attorney and expert/consultant fees incurred in this action.

10. For injunctive relief.

11. Such other and further relief as this Court deems just and equitable.

DATED: November 11, 2022

SOCIAL MEDIA VICTIMS LAW CENTER PLLC

By: _____

Laura Marquez-Garrett (SBN 221542)
Laura@socialmediavictims.org
Matthew P. Bergman (*Pro Hac Vice* anticipated)
matt@socialmediavictims.org
Glenn S. Draper (*Pro Hac Vice* anticipated)
glenn@socialmediavictims.org
SOCIAL MEDIA VICTIMS LAW CENTER
821 Second Avenue, Suite 2100
Seattle, WA 98104
Tel: (206) 741-4862 Fax: (206) 957-9549

WATERS, KRAUS & PAUL
Kevin M. Loew (SBN 238080)
kloew@waterskraus.com
222 North Pacific Coast Hwy, Suite 1900
El Segundo, California 90245
Tel: (310) 414-8146 Fax: (310) 414-8156

SEEGER WEISS LLP
Christopher A. Seeger (*Pro Hac Vice* anticipated)
cseeger@seegerweiss.com
Christopher Ayers
cayers@seegerweiss.com
55 Challenger Road
Ridgefield Park, NJ 07660
Tel: 973-639-9100 Fax: 973-679-8656

Robert H. Klonoff (*Pro Hac Vice* anticipated)
klonoff@usa.net
2425 S.W. 76th Ave.
Portland, Oregon 97225
Tel: (503) 702-0218 Fax: (503) 768-6671

Attorneys for Plaintiffs

EXHIBIT B

A DIGITAL PANDEMIC: UNCOVERING THE ROLE OF 'YAHOO BOYS' IN THE SURGE OF SOCIAL MEDIA-ENABLED FINANCIAL SEXTORTION TARGETING MINORS

PRESENTED BY

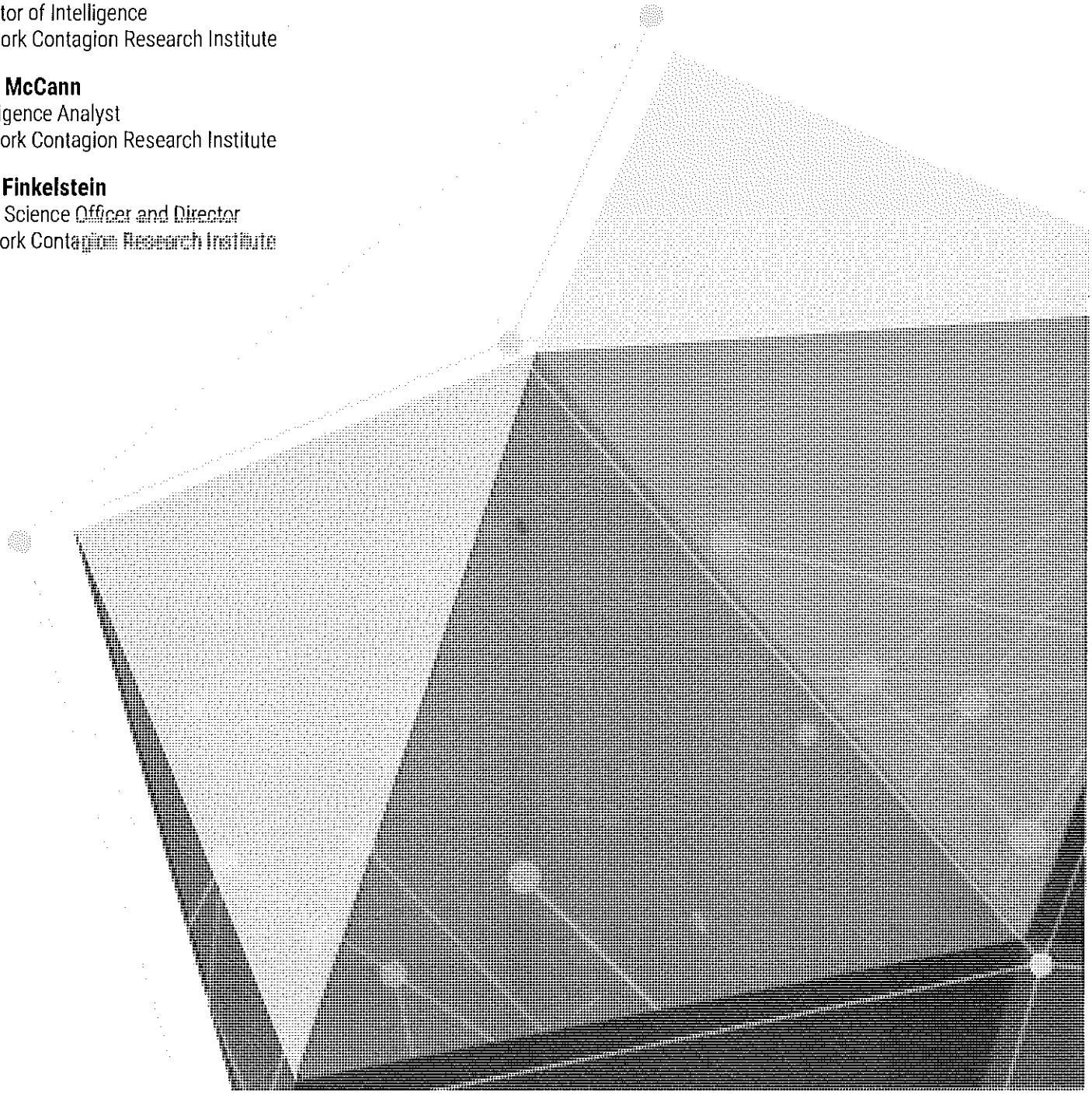
NCRI
NETWORK CONTAGION RESEARCH INSTITUTE

Paul Raffile
Senior Intelligence Analyst
Network Contagion Research Institute

Alex Goldenberg
Director of Intelligence
Network Contagion Research Institute

Cole McCann
Intelligence Analyst
Network Contagion Research Institute

Joel Finkelstein
Chief Science Officer and Director
Network Contagion Research Institute



NCRI
NETWORK CONTAGION RESEARCH INSTITUTE

Threat Intelligence Report

A Digital Pandemic: Uncovering the Role of 'Yahoo Boys' in the Surge of Social Media-Enabled Financial Sextortion Targeting Minors

Financial sextortion is the fastest growing crime targeting children in North America and Australia—accelerating at an alarming rate, with incidents surging up 1,000% in the past 18 months. In a December 2023 hearing, FBI Director Wray warned Congress that sextortion is "a rapidly escalating threat," and teenage victims "don't know where to turn."[1]

Cybercriminals are using fake social media accounts to coerce victims, almost all of them boys, into sharing an explicit photo.[2] As soon as the criminal receives the photo, they threaten to (and sometimes do) expose the photo to the victim's friends, family, and followers unless a ransom is paid. These criminals employ ruthless tactics to intimidate their victims, inflicting lasting trauma and immense distress–which has led to more than 21 youth suicides.[3] [4]

This report reveals that virtually all of the financial sextortion targeting minors today is directly linked to a distributed West African cybercriminal group called the **Yahoo Boys.** Additionally, this investigation unveils previously unreported views into the social media platforms where these criminals share their sextorion scripts, tools, and methods, which has allowed this crime to proliferate at an exponential rate.

Most recently, in November 2023, Olamide Oladosu Shanu, a Nigerian national, was indicted along with four co-conspirators in the largest known financial sextortion operation to date.[5] The indictment alleges that Shanu's criminal enterprise received upwards of $2.5 million U.S. dollars in Bitcoin from victim payments.[6]

[1] https://www.nbcrightnow.com/national/sextortion-is-a-rapidly-escalating-threat-fbi-director-says/video_4fb28c88-04ba-5131-89f3-082396fca798.html
[2] https://www.protectchildren.ca/en/press-and-media/news-releases/2022/sextortion-data-analysis
[3] https://www.missingkids.org/blog/2023/financial-sextortion-growing-crisis
[4] https://www.cbc.ca/news/canada/british-columbia/police-link-suicide-of-12-year-old-prince-george-b-c-boy-to-online-sexual-extortion-1.7041185
[5] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[6] USA v. Shanu (2023) | Case 1:23-cr-00296-BLW via PACER

Key Takeaways:

- Financial sextortion is the most rapidly growing crime targeting children in the United States, Canada, and Australia.
- Nearly all of this activity is linked to West African cybercriminals known as the Yahoo Boys, who are primarily targeting English-speaking minors and young adults on **Instagram**, **Snapchat**, and **Wizz**.
- The tenfold increase of sextortion cases in the past 18 months is a direct result of the Yahoo Boys distributing sextortion instructional videos and scripts on **TikTok**, **YouTube**, and **Scribd**, enabling and encouraging other criminals to engage in financial sextortion.
- The sextortion criminals are "**bombing**" high schools, youth sports teams, and universities with fake accounts, using advanced **social engineering tactics** to coerce their victims into a compromising situation.
- **Generative Artificial Intelligence** apps are already being used to target minors in a fraction of sextortion-at-scale operations.

These findings enhance our understanding of this emerging cyber threat and pave the way for more effective countermeasures to disrupt these cybercriminals. Additionally, the insights from this analysis form a basis for evidence-based policymaking and the development of prevention and support initiatives for victims.

Financial sextortion is the most rapidly growing crime targeting American, Canadian, and Australian youth.

The Network Contagion Research Institute (NCRI) has observed an exponential increase in sextortion cases targeting minors and youth on social media platforms over the past 18 months. During this period, the FBI reported a 1,000% increase in financial sextortion incidents,[7] while NCMEC reported a 7,200% increase in financial sextortion targeting children from 2021 to 2022.[8] This surge has been characterized by the FBI Director and international partners as a "global crisis that demands everyone's attention" [9]

[7] https://apnews.com/article/fbi-online-sexual-extortion-social-media-michigan-2a1fbfc0568fcb0d67da5474b22909f0
[8] https://www.weprotect.org/global-threat-assessment-23/data/
[9] https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis

To date, there have been at least 21 youth suicides linked to this sextortion surge—but this figure is likely a significant underreporting, given the shame and fear that prevent many victims from ever telling anyone about the incident.[10] [11]

For comparison, in a 2018 nationwide survey in the United States, 5% of teens had reported being a victim of sextortion online.[12] By the summer of 2023, 51% of Gen Z teens and young adults said they or their friends were catfished in online sextortion scams resulting in their intimate photos being used against them[13]—and half (47%) of respondents said they or their friends had been targeted in the past 3 months.[14]

According to Snapchat internal data, 31% of teens who are approached by a sextortion criminal ultimately share a compromising photo.[15] [16]

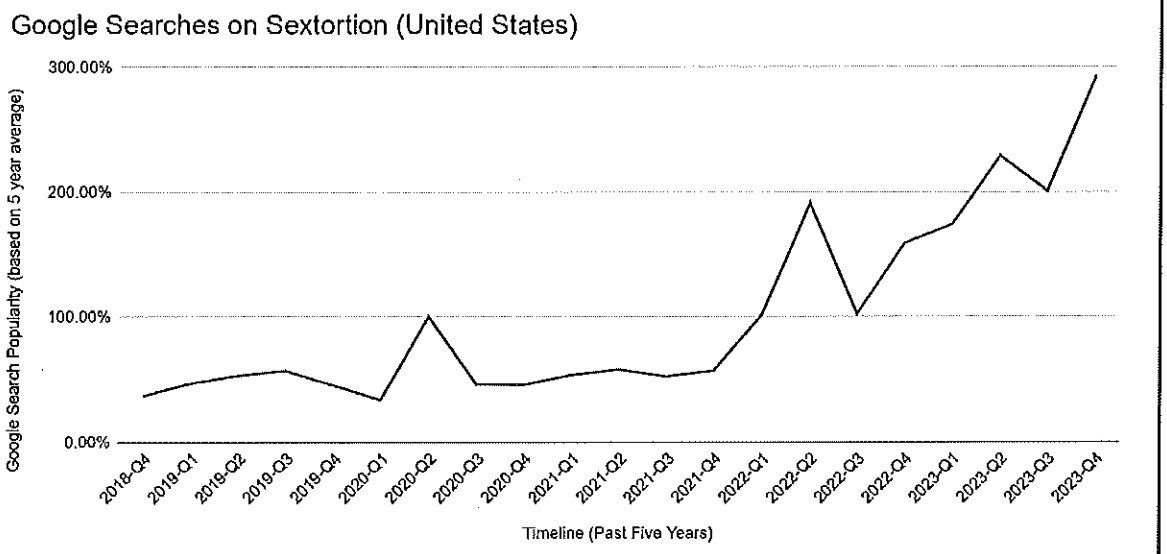
In the **United States**, the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), and the National Center for Missing and Exploited Children (NCMEC) issued a national Public Safety Alert on the "explosion" of sextortion incidents targeting teens.[17] At the time of this writing, NCMEC has received more than 20,000 reports related to financial sextortion.[18]

In **Canada**, the Canadian Centre for Child Protection's Cybertip program currently receives an average of 50 sextortion reports per week,[19] calling it "an unprecedented volume"[20] and "a public safety emergency." Several recent tragedies in Canada have sparked renewed calls for child safety regulation on social media platforms. In October 2023, a 12 year old boy in British Columbia died by suicide after being sextorted on Snapchat and Instagram.[21] Another 17 year old from Manitoba died last year only three hours after he was targeted by the sextortion criminal.[22]

In **Australia**, the Federal Police say they've seen sextortion cases grow by 300% in the past year and now receive about 300 complaints per month—although authorities estimate only 1 in 10 victims actually report the crime to police.[23] [24] [25]

[10] https://www.missingkids.org/blog/2023/financial-sextortion-growing-crisis
[11] https://www.cbc.ca/news/canada/british-columbia/police-link-suicide-of-12-year-old-prince-george-b-c-boy-to-online-sexual-extortion-1.7041185
[12] https://journals.sagepub.com/doi/full/10.1177/1079063218800469
[13] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/
[14] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/
[15] https://www.foxbusiness.com/technology/sextortion-schemes-target-two-out-every-three-teens-snap-research-shows
[16] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/
[17] https://www.cbsnews.com/video/financial-sextortion-scams-targeting-teen-boys/
[18] https://www.missingkids.org/blog/2023/financial-sextortion-growing-crisis
[19] https://www.cybertip.ca/en/online-harms/sextortion/
[20] https://www.cbc.ca/news/canada/british-columbia/sextortion-recovery-scams-1.6774652
[21] https://www.cbc.ca/news/canada/british-columbia/police-link-suicide-of-12-year-old-prince-george-b-c-boy-to-online-sexual-extortion-1.7041185
[22] https://www.cbc.ca/news/canada/manitoba/manitoba-sexploitation-suicide-1.6494054
[23] https://www.theguardian.com/australia-news/2023/nov/09/australia-federal-police-facebook-meta-young-people-scams-esafety
[24] https://www.abc.net.au/listen/programs/illawarra-breakfast/helen-schneider/103163730
[25] https://www.abc.net.au/news/2023-10-22/snapchat-extortion-explicit-photo-victim-speaks-out/102932958

It's worth emphasizing that the percentage of victims who ultimately report the incident to authorities is low, given the shame and fear that many victims experience.[26] These organizations recognize their metrics are likely only the tip of the iceberg. To better understand the larger scale at which financial sextortion is occurring, two additional sources may be examined. The first measure is a surge of Google Searches about sextortion and highly-correlated search inquiries expected of new victims. The second is the exponential growth of the world's largest sextortion support community.

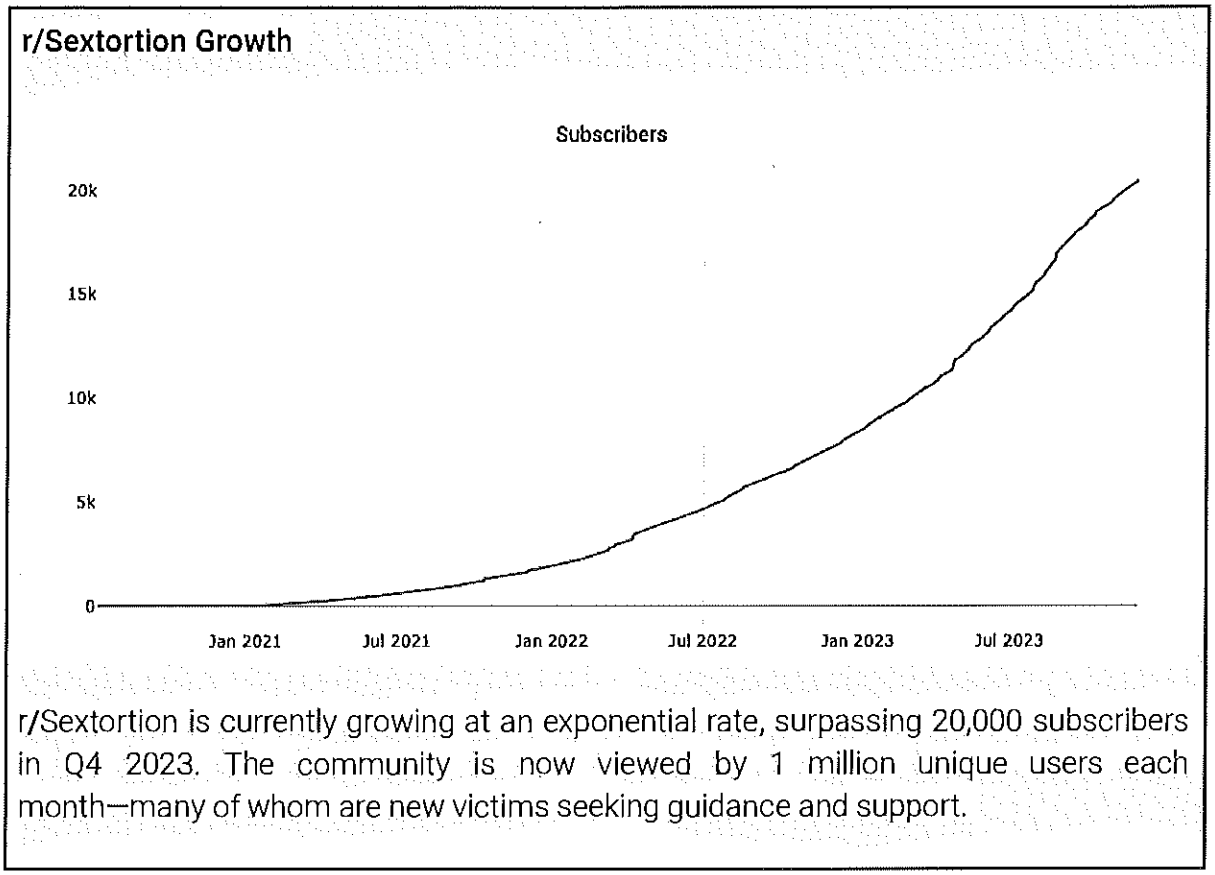


The staggering amount of Google searches related to sextortion is largely driven by new victims seeking help for their situation. Closely related search queries by similar users include "how to delete Instagram account" and "how to report sextortion".[27]

r/Sextortion is the world's largest sextortion support forum. This Reddit community was created in February 2020 and, at the time of this report, has more than 20,000 members (subscribers) and surpassed 1 million monthly unique viewers in November 2023.[28] It is now among the Top 5% largest Reddit communities.[29] Members who author posts or comments in the forum are nearly always victims of financial sextortion seeking support or offering advice.[30] The moderated forum creates a safe haven for victims to give and receive support. Its growth highly suggests an exponential growth in victimization rates

[26] https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf
[27] https://trends.google.com/trends/explore?date=today%205-y&geo=US&q=sextortion&hl=en-US
[28] https://www.reddit.com/r/Sextortion/
[29] Ibid.
[30] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

and the forum provides insight into some of the methods and tactics used by the criminals.



r/Sextortion is currently growing at an exponential rate, surpassing 20,000 subscribers in Q4 2023. The community is now viewed by 1 million unique users each month—many of whom are new victims seeking guidance and support.

Instagram, Snapchat, and Wizz are the leading platforms where youth are being targeted by financial sextortion.

According to the most recent NCMEC data, minors are most often victimized by sextortion on the following apps.[31]

- **Instagram** is the most common vector that sextortion criminals use to target their victims. Instagram's design and features make it the most accessible platform for blackmailers to quickly attain personal information about the victim to initiate a successful sextortion attack. Specifically, nearly all financial sextortion attacks on minors involve the screenshotting of the victim's Instagram followers/following lists and using those lists as leverage, threatening to send the victim's intimate

[31] https://www.nbcnews.com/tech/social-media/friend-finding-app-offered-safe-space-teens-sextortion-soon-followed-rcna91172

photos to all these accounts. Unlike Meta's Facebook, where users can opt to make their connections private, Instagram does not offer this privacy safeguard.

- **Snapchat** is most frequently utilized to coerce victims into sending a compromising photo. While the conversation may start on Instagram or Wizz, the criminals usually direct victims to Snapchat to exchange photos. Snapchat is the preferred app by criminals because its design features provide a false sense of security to the victim that their photos will disappear and not be screenshotted. Criminals effectively exploit Snapchat's safety features that are intended to keep users safe, circumventing the screenshot notification feature, and Snapchat's "live photo" indicator despite using a prerecorded video.

- **Wizz** is the third-most prevalent, but fastest rising social media platform for sextortion of minors.[32] This trending app has similar features to Tinder, but is marketed towards children 13+ and has been downloaded 15 million times.[33] In a poll of 500 English-speaking Wizz users, 40% reported being sextorted on Wizz. Among those victims, 77% of them are minors.[34] Some victims report being targeted by sextortion within minutes of joining the app, suggesting that criminals have saturated Wizz.[35] In the Google Play Store and the App Store, dozens of minors have reported that they were coerced into producing self-generated child sexual exploitation material (SG-CSEM) and blackmailed on Wizz[36]—alongside other child safety concerns, including a high frequency of complaints that the app is serving pornographic ads to minors.[37] Wizz is owned by French appmaker Voodoo[38] and does not report incidents of child sexual exploitation on its platform to NCMEC.

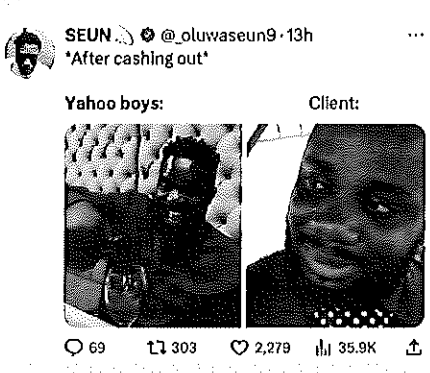
These alarming trends and statistics beg the question: what has caused financial sextortion to skyrocket over the past 18 months?

[32] https://www.nbcnews.com/tech/social-media/friend-finding-app-offered-safe-space-teens-sextortion-soon-followed-rcna91172
[33] https://apps.apple.com/us/app/wizz-app-chat-now/id1452906710
[34] https://www.reddit.com/r/Wizz_app/comments/15bt3v1/have_you_been_blackmailed_over_nudes_on_wizz/
[35] https://www.reddit.com/r/Sextortion/comments/18679it/help/
[36] https://play.google.com/store/apps/details?id=info.wizzapp&hl=en&gl=US
[37] https://apps.apple.com/us/app/wizz-app-chat-now/id1452906710
[38] https://www.voodoo.io/apps

West African cybercriminals known as the "Yahoo Boys" are responsible for the surge of the financial sextortion targeting minors on Instagram, Snapchat, and Wizz.

The exponential increase of sextortion cases is driven by the Yahoo Boys, a financially-motivated, distributed group of overseas cybercriminals[39], adopting this tactic as a primary method of financial gain. The Yahoo Boys, nicknamed after their use of Yahoo.com emails to conduct phishing scams decades ago,[40] are a distributed group of cybercriminals, mostly in Nigeria, who have been associated with many online scams.[41] [42] They are the original "Nigerian Princes", who have shifted in recent years to conduct elderly fraud, fake job scams, romance scams[43]—and now the mass sexual extortion of children for profit.[44]

The Yahoo Boys are a major threat actor, actively targeting youth in the United States, Canada, United Kingdom, Australia, Europe, and elsewhere.[45] The Yahoo Boys openly share their tactics and tradecraft among their social media networks, which has resulted in the alarming uptick in sextortion cases and subsequent suicides.



1.

2.

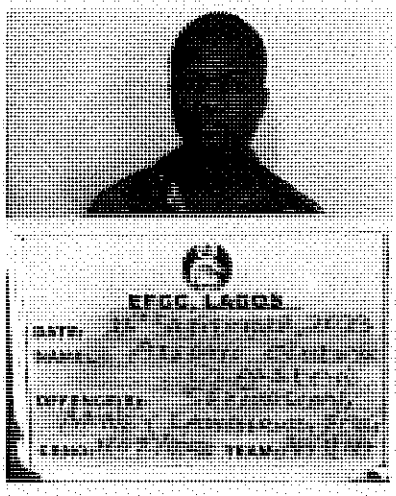
Photo 1 This meme posted on X (formerly Twitter) depicts a representation of a Yahoo Boy and his "client" (victim) after cashing out from a scam.

Photo 2 This TikTok depicts a self-identified Yahoo Boy creating a meme of his experience as a sextortion criminal, and makes reference to blackmailing a "client" (victim) over their nudes.

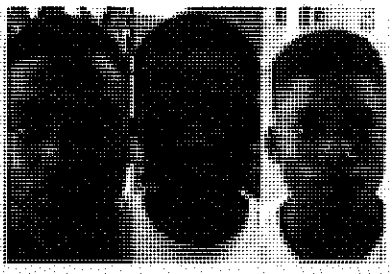
[39] https://www.proquest.com/docview/1350307576?sourcetype=Scholarly%20Journals
[40] https://therecord.media/for-a-former-yahoo-boy-romance-is-a-cut-and-paste-proposition
[41] https://www.proquest.com/docview/1350307576?sourcetype=Scholarly%20Journals
[42] https://longreads.com/2023/07/11/inside-the-world-of-nigerian-yahoo-boys-atavist-excerpt/
[43] https://www.walshmedicalmedia.com/open-access/narrative-of-illicit-money-yahoo-boy-format-of-cyber-scams-and-governance-challenges-in-africa.pdf
[44] https://www.foxnews.com/us/expert-warns-growing-social-media-sextortion-schemes-targeting-boys
[45] https://www.theguardian.com/australia-news/2023/nov/09/australia-federal-police-facebook-meta-young-people-scams-esafety

The Yahoo Boy subculture has become a part of the Nigerian internet landscape.[46] These individuals are known for their lavish lifestyles fueled by ill-gotten gains. The subculture is often associated with flaunting wealth, displaying expensive items like cars, designer clothes, and jewelry on social media to showcase their success.[47]

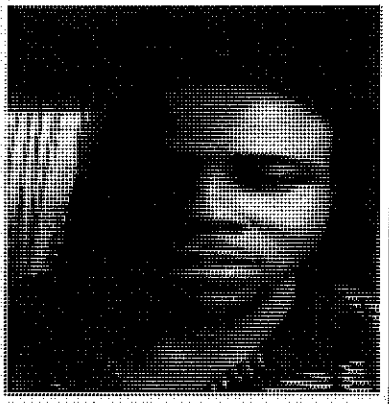
There has been little published about the criminals involved in the current financial sextortion surge. To date, there are only three known indictments of these criminals in court records and public reporting. In August 2023, two Nigerian men were extradited to the United States for sextorting numerous American boys, and causing the death of 17 year old Jordan DeMay[48]; local reporting in Nigeria identified them and four other co-conspirators as Yahoo Boys.[49] In September 2023, Nigeria's Economic and Financial Crimes Commission arrested a man for the sextortion of a 14 year old Canadian boy who died by suicide.[50] Most recently, in November 2023, Olamide Shanu and unidentified co-conspirators in Nigeria, were indicted for receiving more than $2.5 million dollars in Bitcoin transactions amid a large-scale financial sextortion operation.[51]



Olukeye Adedayo Olalekan was arrested in September 2023 for his role in the sextortion of a 14 year old Canadian boy who died by suicide.



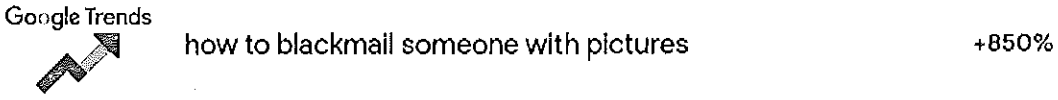
In August 2023, three men from Nigeria were extradited to the U.S. for their involvement in sextortion schemes targeting American boys, which led to the death by suicide of 17 year old Jordan DeMay.

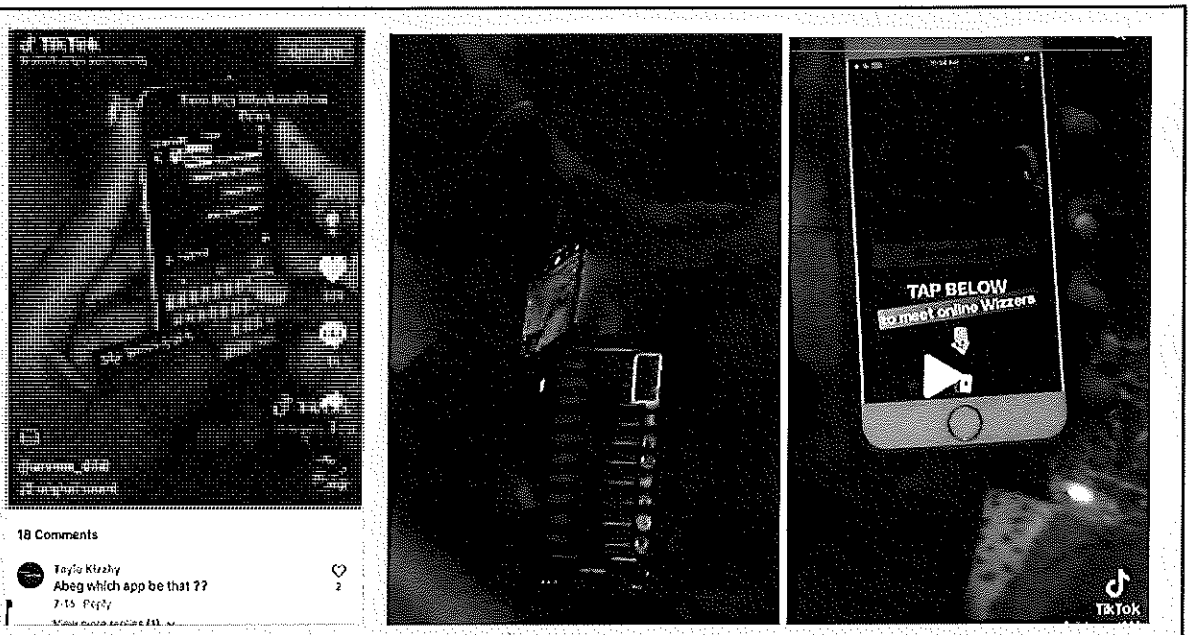


Olamide Oladosu Shanu was indicted in November 2023 for his role in a financial sextortion conspiracy that involved more than two million dollars paid by victims.

[46] https://www.researchgate.net/publication/343432593_Social_Values_and_the_Yahooboys'_Subculture_in_Nigeria_Towards_A_Paradigm_Shift_for_National_Value_Re-Orientation
[47] https://www.cybercrimejournal.com/pdf/adebusuyiijccdec2008.pdf
[48] https://www.justice.gov/usao-wdmi/pr/2023_0813_Two_Nigerian_Men_Extradited_To_The_United_States
[49] https://gazettengr.com/sextortion-fbi-hails-efcc-for-nabbing-six-yahoo-boys-tied-to-suicide-of-american-teenager/
[50] https://www.efcc.gov.ng/efcc/news-and-information/news-release/9496-efcc-arraigns-man-for-alleged-sextortion-in-lagos
[51] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER

According to Google Search Trends in Nigeria, the phrase "how to blackmail someone with pictures" is trending up 850% at the time of this writing.[52]





Dozens of videos posted to TikTok and YouTube show individuals self-identified as Yahoo Boys actively engaged in sextorting minors on Instagram, Snapchat, and Wizz.

> The Yahoo Boys are widely sharing sextortion scripts and instructional videos on TikTok, YouTube, and Scribd, encouraging other criminals to partake in sextortion.

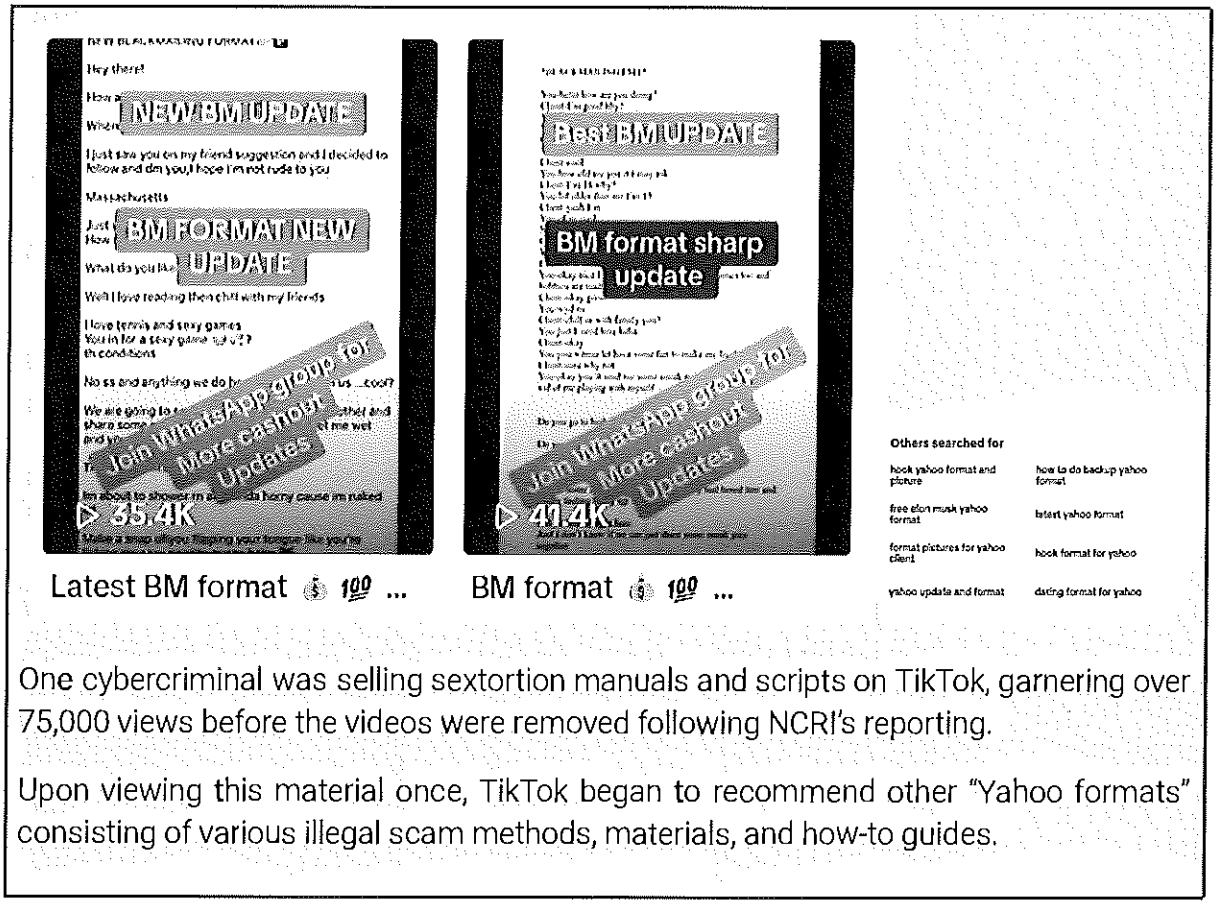
These sextortion scripts have been viewed more than half a million times on **TikTok**, **YouTube**, and **Scribd**. Comments on these videos are filled with criminals eagerly asking to download the sextortion script and tools. Most of the comments on these videos appear to be other from cyber scammers, often commenting in Nigerian Pidgin dialect.

[52] https://trends.google.com/trends/explore?geo=NG&q=how%20to%20blackmail&hl=en-US

These videos and scripts are publicly accessible under the titles "**Blackmail Format**" and "**BM Format**". These posts often using the tags **#YahooBoys**, **#YahooFormat**, **#YahooUpdates**, and **#ElonMuskBoys** to connect with others within this group.

Yahoo Boys refer to their victims as **"clients"**, a term they use to evade getting banned on social media platforms.

These videos provide detailed instructions and incentives for other cybercriminals to engage in financial sextortion against minors.

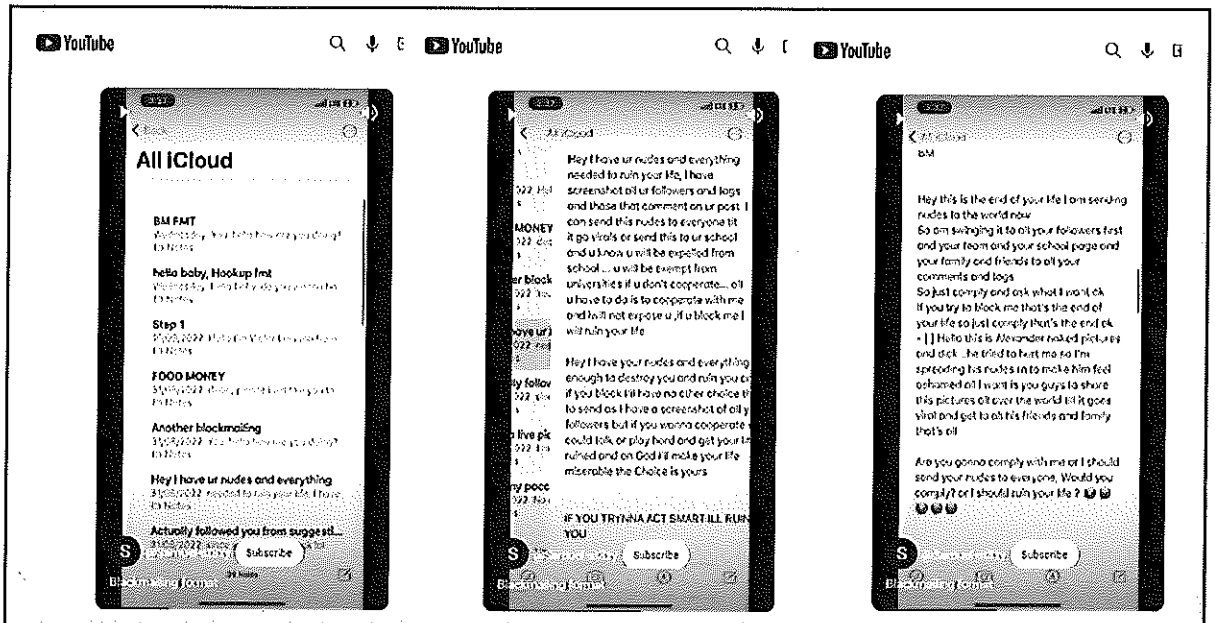


Latest BM format 💰 💯 ... BM format 💰 💯 ...

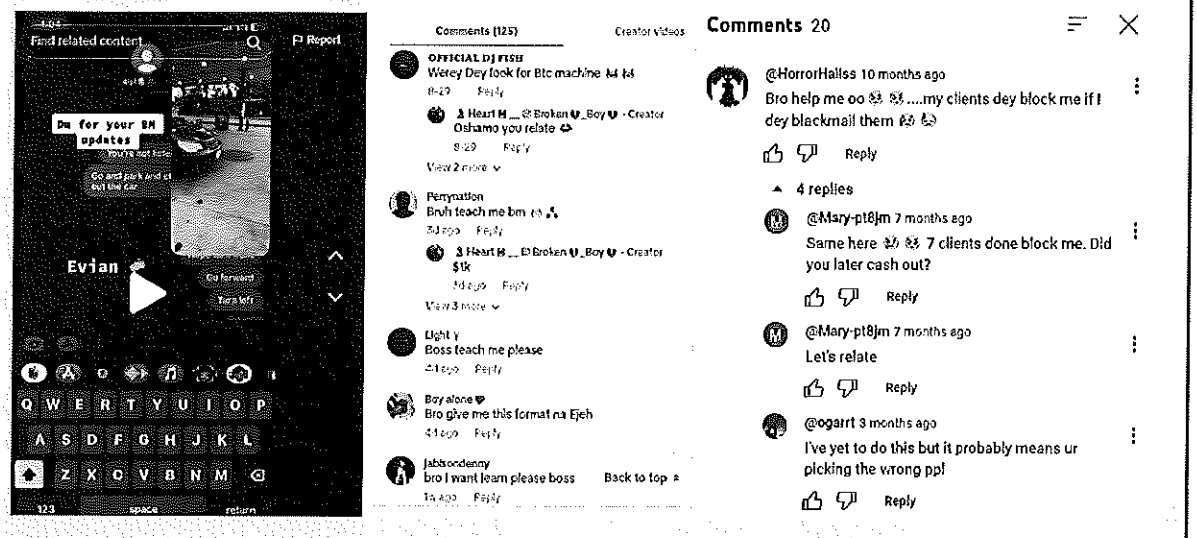
One cybercriminal was selling sextortion manuals and scripts on TikTok, garnering over 75,000 views before the videos were removed following NCRI's reporting.

Upon viewing this material once, TikTok began to recommend other "Yahoo formats" consisting of various illegal scam methods, materials, and how-to guides.

All sextortion manuals and scripts identified during this investigation were linked to the Yahoo Boys and nearly all accounts commenting on the videos spoke in Nigerian Pidgin, used slang specific to the same region, or were attributable to the region via an examination of their profile.

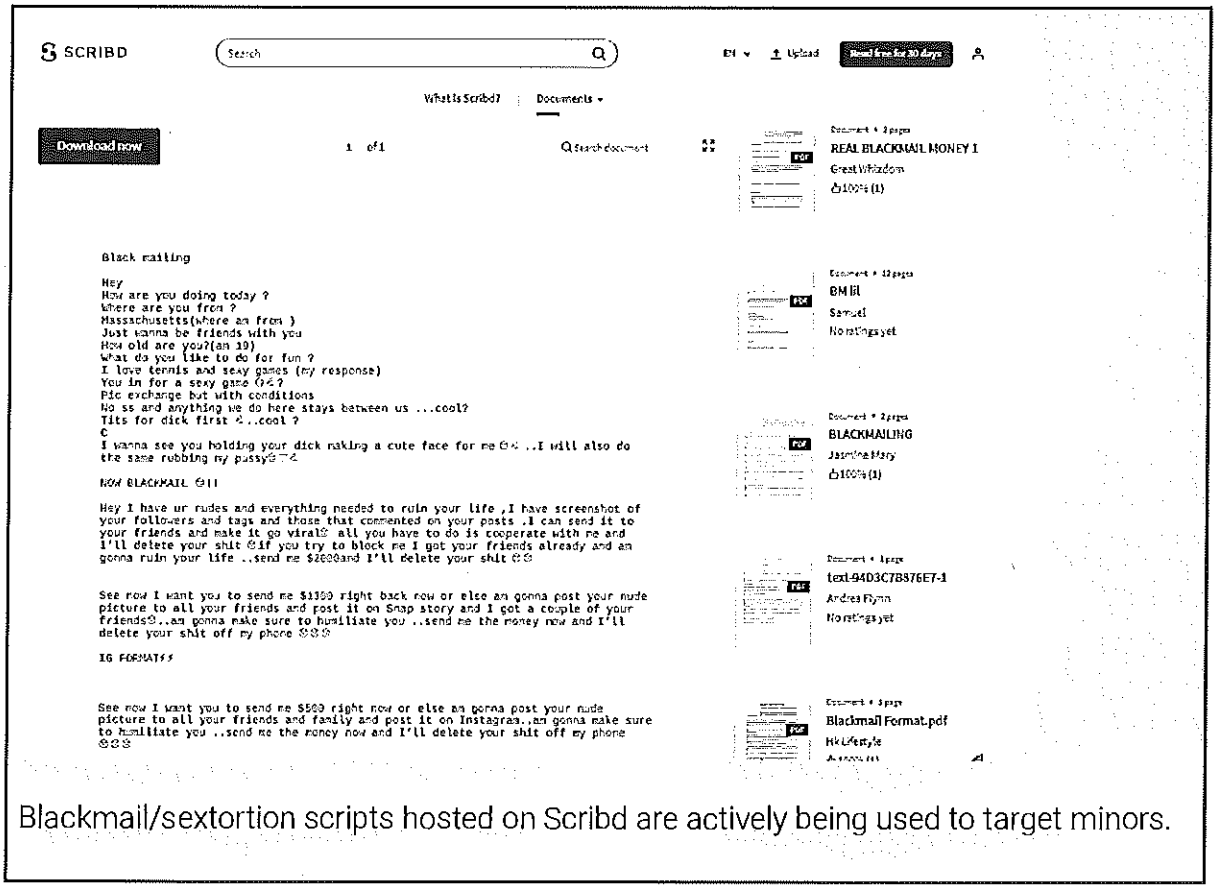


In a series of videos called "Blackmailing format" uploaded to YouTube in September 2022, one cybercriminal shared four sextortion scripts.



The TikTok video on the left shows a sextortion criminal directing his victim to a Bitcoin ATM while requiring the victim to livestream his location; commenters eagerly ask to be taught how to conduct the scam. The comments section of TikTok and YouTube sextortion tutorials serve as a virtual trade show for cybercriminals to share tactics and scam materials.

In addition to video sharing sites like TikTok and YouTube, dozens of sextortion scripts have been shared among cybercriminals using Scribd—a document hosting site. These sextortion scripts have been viewed over 100,000 times in total.

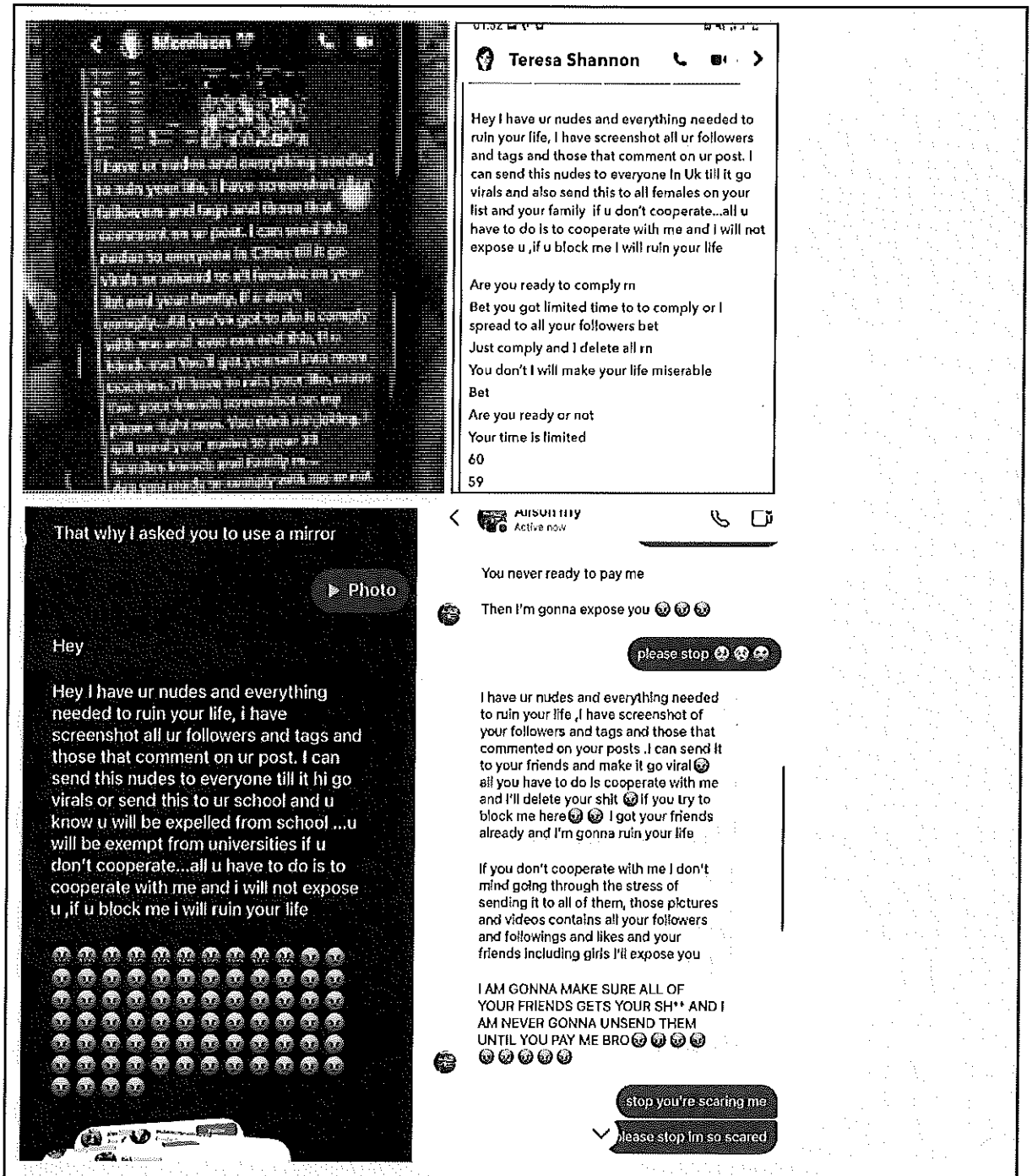


Blackmail/sextortion scripts hosted on Scribd are actively being used to target minors.

Many of the sextortion attacks happening today use the exact scripts that have been circulated in the Yahoo Boy social media networks shown above. NCRI has observed sextortion criminals actively using these scripts against minors in the United States, Canada, United Kingdom, Australia, and the Netherlands.[53] Victims frequently report receiving the same threatening messages, verbatim, in a sextortion support forum.[54]

Despite the most popular sextortion scripts being publicly accessible since 2021, their text has not yet been blacklisted by Instagram, Wizz, or Snapchat—as these scripts are actively being used today against victims. USA v. Shanu court filings show these exact materials being used against minors.[55]

[53] https://www.reddit.com/r/Sextortion/
[54] https://www.reddit.com/r/Sextortion/
[55] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER



Victims share their experiences in r/Sextortion, a community support forum. The same sextortion scripts that have been circulating in Yahoo Boy social media networks are actively being used against minors at massive scale on Instagram, Wizz, and Snapchat.

> The sextortion criminals are "**bombing**" high schools, sports teams, and universities with fake accounts, using advanced **social engineering tactics** to coerce their victims into a compromising situation.

The sextortion guides on TikTok and YouTube provide step-by-step instructions to create convincing fake social media profiles and how to "**bomb**" high schools and sports teams.[56] The Yahoo Boys use this term to describe friending/following as many people in a school or target location as possible.[57] In many cases of sextortion, the victim believes the individual is potentially an unknown classmate or someone of the same age from a neighboring town. For example, the criminal who drove 15 year old Riley Basford to suicide in 2021 had fifteen mutual followers.[58]

Sextortion "formats" are detailed how-to guides that are shared among Yahoo Boy cybercriminals on TikTok and YouTube. They provide step-by-step instructions on how to create fake accounts, obtain a texting number, how to target victims with the scam, and cash out. They show how criminals should target high schools and also provide instruction on threats to use against the victims.

[56] https://sports.yahoo.com/rugby-players-among-athletes-becoming-201540323.html
[57] https://journalasap.org/index.php/asap/article/view/26/28
[58] https://www.insideedition.com/15-year-old-takes-his-own-life-after-falling-victim-to-internet-blackmailing-ploy-family-says-66294

Tactics, Techniques & Procedures

The numerous sextortion how-to guides on TikTok, YouTube, and Scribd direct the criminals through the steps to conduct a successful financial sextortion operation.

The criminals exploit the **platform design** and **features** of three major applications where they have unfettered access to youth. When their accounts are banned, they buy or create new accounts with impunity and/or factory reset their phones to evade app bans.

Instagram

- The criminals "bomb" high schools, sports teams, and other youth groups with follow requests in order to appear to have many mutual friends with their targets.
- The moment an Instagram user accepts the follow request of a scam account, their follower/following list is compromised. This gives criminals easy access to the target's followers and following lists to use as blackmail, threatening to send the compromising photos to all these acquaintances. With Instagram's current configuration, users have no way to protect themselves against their followers and following lists being copied the instant they accept a follow request.

Snapchat

- Sextortion criminals often exploit Snapchat to send pre-recorded videos of attractive females as "live" snaps (purple/red icons). Generally, pre-recorded videos and photos are shared with a blue icon. This feature exploitation gives victims a false sense of security that the Snaps they are receiving are real-time images.
- Criminals are also able to bypass the Snapchat feature that notifies users when a screenshot has been taken of their Snaps. In the absence of this notification, victims believe their images have not been screen-recorded or screenshotted.
- Additionally, Snap Scores are perceived by victims as an indicator of authentic account activity. The higher the Snap Score, the more history the account has on the platform. Criminals are inflating Snap Scores on their accounts using bot activity, automated scripts[59], and using hacked accounts with preexisting Snap Scores in order to appear as an authentic profile.[60]

Wizz

- Victims have reported being targeted nearly immediately upon account creation (in some cases within ten minutes),[61] suggesting the platform is saturated by sextortion activity.

[59] https://github.com/useragents/Snapchat-Snapscore-Botter
[60] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[61] https://www.reddit.com/r/Sextortion/comments/18679it/help/

- In order to reach as wide an audience as possible, cybercriminals are using two methods to "match" with thousands of potential targets. First, Wizz users can boost their profile for a small fee. Second, criminals employ the use of VPNs to spoof their location to numerous target regions.

Social Engineering

These criminals and their catfish accounts are extremely manipulative and convincing. According to Snapchat's internal data, approximately one third of the youth who engage with a sextortion criminal end up sending a compromising photo, resulting in a blackmail incident.[62]

In order to wield extremely convincing catfish accounts, the criminals are often using stolen and hacked Instagram accounts, which give the appearance of an authentic profile, also known as "aged" accounts. They have a history of authentic activity, posts, followers, and other characteristics that make detecting the catfish profile much more difficult. Aged accounts also bypass a number of moderation and safety controls, while newly created accounts appear more likely to be taken down when reported.

After establishing contact with a target, sextortion criminals use established techniques, operating under false pretenses and employing sophisticated emergent technologies including generative AI, to coerce victims, many of whom are underage, to share nude photos of themselves in compromising situations.

To conduct the sextortion scam, criminals tend to use files of amateur, self-produced imagery, sometimes stolen or bought from OnlyFans models, adding to the apparent authenticity of the account.

Extreme Threats & Coercion

Immediately after a victim shares an explicit photo, their extortionist uses an established script that is shared widely among Yahoo Boys on social media. This script takes advantage of a victim's embarrassment at the threat of exposure of their explicit photo(s). Oftentimes, these scripts include extreme threats and coercion:[63]

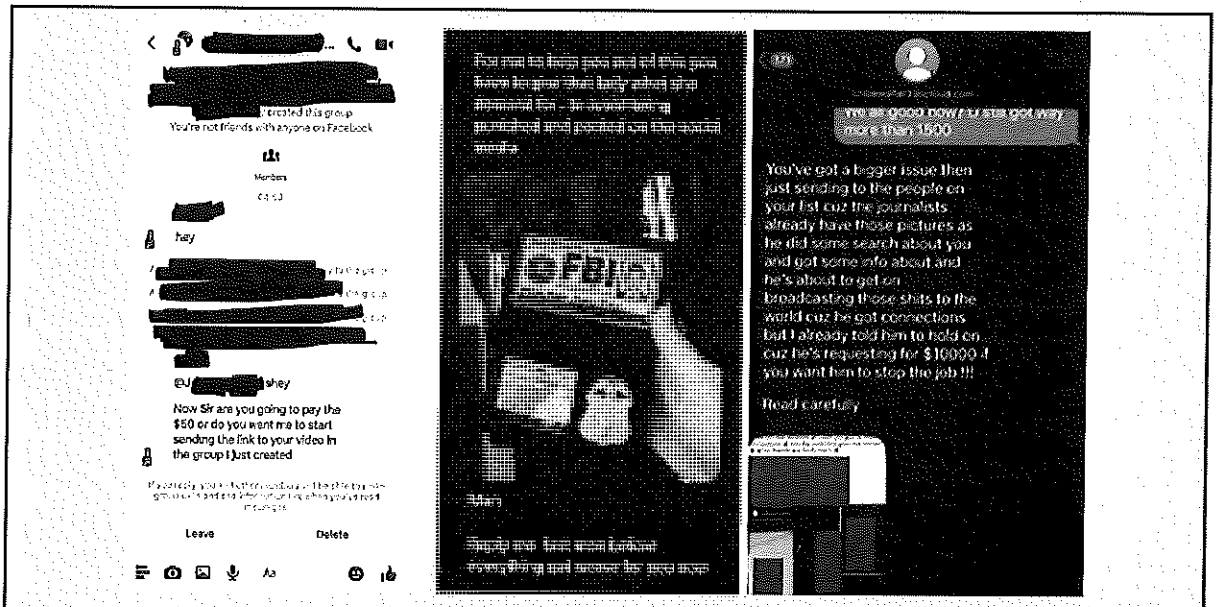
- Sharing screenshots of a victim's Instagram followers and following lists to establish that the criminal can share the photos with all the individuals in the victim's social network.
- Sending screenshots of draft messages to the victim's friends or family.
- Claiming that they will frame the victim for sending nude pictures to a child.
- Creating a "wanted" posted with the victim's nude images, name, and number.

[62] https://www.foxbusiness.com/technology/sextortion-schemes-target-two-out-every-three-teens-snap-research-shows
[63] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

- Threatening that the photos being shared will result in the victim being expelled from school, exposed to criminal action, unable to attend college, or that their parents will be fired from their jobs.
- The criminals sometimes begin sending the photos to Instagram group chats with the victim and some of the victim's contacts. Since the victim is in this group chat, the criminal tries to persuade payment in order to un-send the photos before others see the message.

Aggressive Cyber Stalking Tactics

Sextortion criminals also employ ruthless tactics amounting to cyber stalking.[64] They use multiple accounts to continually harass victims on social media. They barrage victims with incessant texts and iMessages from many different phone numbers. On occasion, criminals will contact friends and family members, asking to be put in contact with the victim. Data aggregators and people databases are common tools of the sextortion criminals. They search these databases to find their victims' address, photos of their home, their relatives and known associates, and sometimes their phone numbers. These elements intensify the threats against victims. Sometimes the schemes involve a different phone number, pretending to be law enforcement, offering to "settle" the case with a monetary sum. In some cases, this harassment can continue for months.



Sextortion criminals threaten to expose illicit photos in group chats made with victims' family members or friends. They also operate under false pretenses, sometimes posing as law enforcement agents or journalists.

[64] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER

Payments in Perpetuity

Sextortion criminals often start with a single demand: "pay me now and the photos will be deleted." However, if the victim pays, the photos aren't deleted and the criminals continue to demand multiple payments over an extended period. This is why the prevailing guidance from law enforcement is to immediately block the criminal and do not pay.

If the victim pays, it's common for victims to be put on scheduled payment plans with a ransom payment due weekly or monthly.[65]

Sextortion criminals often ask victims to purchase gift cards or make payments via Cashapp, Venmo, iTunes, Steam, or gift cards.[66]

[65] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[66] https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

Victims as Forced Accomplices, Money Mules & Account Creators

If victims cannot afford payments, the criminals often request victims to hand over their social media accounts or create new accounts for the criminal to use in the furtherance of the scam.

The NCRI has also observed that sextortion criminals sometimes demand that victims create fraudulent accounts on websites like Login.gov and IRS.gov, in the furtherance of other fraudulent activity.

U.S. citizens are used as intermediaries, or 'money mules', to transfer funds to sextortion criminals.[67] Victims have been coerced into acting as money mules facilitating layered transactions, receiving funds from victims and then passing them on to other members of the criminal network. The schemes extensively use peer-to-peer (P2P) payment apps like Venmo and Cashapp, along with gift cards, for initial fund transfers. Cryptocurrency is also often used.[68]

Artificial Intelligence and deepfake nude apps are already being used to target minors in widespread financial sextortion-at-scale operations.

Generative artificial intelligence ("AI") software is already being used to conduct a growing number of the financial sextortion-at-scale attacks against minors, and the likelihood of abuse will become considerably greater in coming months as generative AI technologies become more realistic and convincing.[69]

There are two distinct methods by which AI is being used in sextortion operations:

1. To generate artificial nude photos of someone, through which to extort payment
2. To create more convincing "catfish" profiles than ever before

AI Generated Nude Photos of Non-Consenting Victims for Sextortion

In this newest variant of the sextortion scam, the cybercriminals don't need to coerce the victim to share a compromising photo. All the criminal needs is a fully clothed photograph from Instagram and a clothes-removing AI app to initiate their extortion attack.[70] The

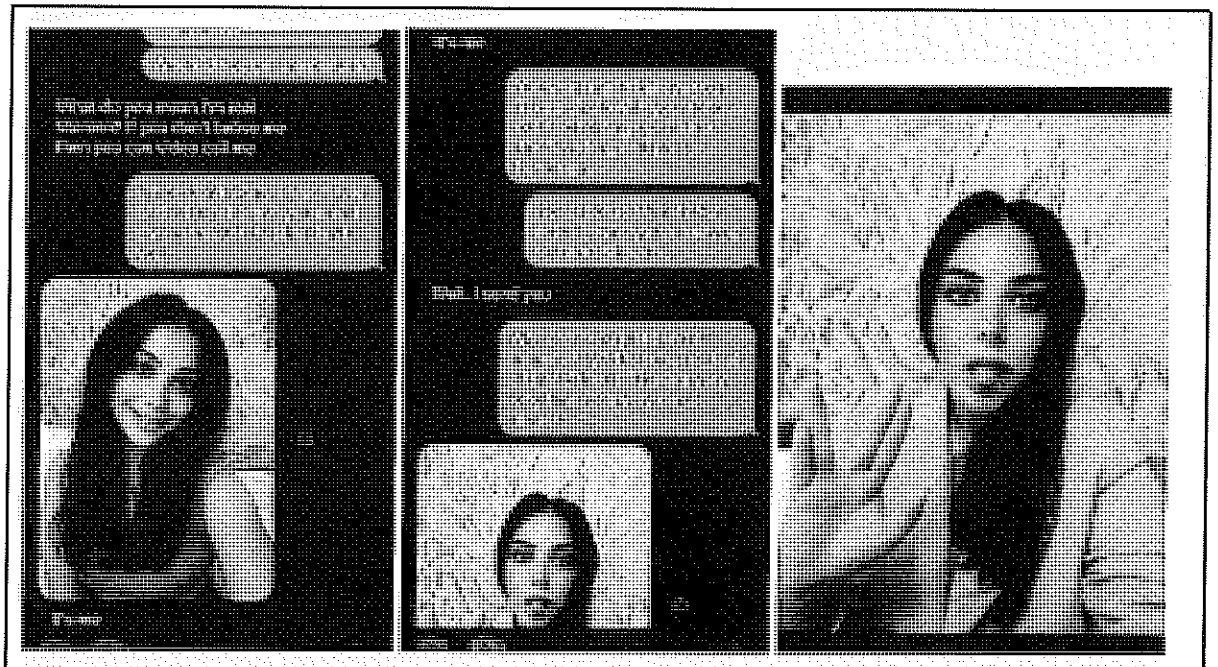
[67] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[68] USA v. Shanu (2023) | Case 1:23-cr-00296-BLW via PACER
[69] https://www.ic3.gov/Media/Y2023/PSA230605
[70] https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

tactics remain the same: the criminal threatens to share the photo with the victim's friends and family, often with an embarrassing accusation, to entice payment.

In June 2023, the FBI published a warning that sextortion criminals manipulate benign photographs or videos to target victims using synthetic images (deepfakes) to extort payment.[71] In the month of October 2022, Crime Stoppers Houston received at least eight reports from Houston-area moms with teenage boys who were targeted with AI generated nude photos of themselves.[72]

There are numerous AI apps, websites, and services that 'nudify' images, generating explicit interpretations of clothed individuals and these apps and services are proliferating across criminal networks.[73] With the growing accessibility of these apps paired with the lack of meaningful safeguards from non-consensual imagery, they are an effective tool for cybercriminals to exploit victims without ever needing to receive a compromising photograph.[74]

AI-Enhanced Catfish Profiles



This conversation between a cybercriminal and a potential victim shows how criminals are effectively using generative AI tools to manipulate photographs to falsely show "proof of life", resulting in a convincing catfish.

[71] https://www.ic3.gov/Media/Y2023/PSA230605
[72] https://www.khou.com/article/news/local/houston-kids-online-sextortion-photos/285-3f18171a-3a2d-47c3-a86f-d34d47416425
[73] https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf
[74] https://www.graphika.com/reports/a-revealing-picture

Numerous videos posted to Yahoo Boy networks on TikTok and YouTube provide instruction about how to exploit AI tools to conduct sextortion and other scams, specifically how to use real-time face swapping software, voice-changers, and using pre-recorded video calls to communicate with their victims.

In light of the escalating use of generative AI in perpetrating financial sextortion, urgent attention and proactive measures are imperative. The documented instances of AI's application in creating deceitful profiles and manipulating multimedia for fraudulent activities are alarming. As these technologies advance, the risk of exploitation amplifies, potentially causing irreparable harm to vulnerable individuals. Mitigating this threat demands a multi-faceted approach encompassing stringent regulation, heightened cybersecurity awareness, and the collaboration of tech platforms to curb the misuse of AI tools. The responsibility falls on both policymakers and technology innovators to proactively address these challenges to safeguard individuals, especially minors, from falling victim to these increasingly sophisticated and damaging cybercrimes.

Outlook

This research has shed light on the factors contributing to the alarming rise in sextortion cases. By delving into the methods employed by criminal entities and unraveling the profound scale and impact on victims, this study has laid a foundation for effective countermeasures to disrupt this crime. The insights garnered here are pivotal in crafting

effective strategies and evidence-based policies aimed at preventing and combating sextortion. Moreover, by dissecting the tactics utilized by criminals, this report underscores the importance of enhanced detection, mitigation, and adjudication of these incidents. Ultimately, this research has focused on understanding how social media features have been exploited by sextortion criminals, shedding light on safety controls and privacy issues. To mitigate this emergent threat, stakeholders in civil society and technology must strive to mitigate the vulnerabilities and misuse of these platforms, offering a pathway towards a safer online landscape.

Recommendations

Recommendations to Social Media Platforms

1. **Instagram should give users the option to set their Followers and Following lists to Private, and set all minors' Followers and Following lists to private by default.**

   One common factor in nearly all sextortion cases reviewed by the NCRI was the cybercriminals' consistent use of the victim's Instagram Followers and Following lists. Using these screenshotted lists, criminals exert immense leverage on victims, threatening to send the material to all of their friends, family, and connections.

   Unlike Meta's other social network, Facebook, Instagram users cannot make their connections private. Because Instagram users cannot make their Followers and Following lists private, extorters have easy access to other users connected to their victim, and the opportunity to craft their accounts to appear more authentic by establishing mutual connections.[75]

   Instagram can mitigate a vast majority of financial sextortion cases by hiding minors' Followers and Following lists on their platform by default,[76] and by giving all users the option to make these lists private. This setting should be decoupled from the setting to make your Instagram photos public or private.

2. **Instagram and Wizz should improve the in-app reporting process to quickly and effectively ban sextortion accounts.**

   In early 2023, Snapchat created a distinct reporting category for sextortion.[77] Instagram, Wizz, and other platforms where financial sextortion occurs should follow suit and ensure that all reports of sextortion are adjudicated by a human

[75] https://protectchildren.ca/en/resources-research/an-analysis-of-financial-sextortion-victim-posts-published-on-sextortion/
[76] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[77] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/

moderator within hours. Victims have repeatedly suggested that Instagram took no action on reports made against sextortion accounts.[78]

3. **Instagram and Snapchat should proactively detect the sextortion scripts and investigate any users who attempt to use them.**

   Identical scripts are being repeatedly deployed at scale on Instagram, Snapchat, and Wizz by accounts linked to sextortion. Identification and detection of these sextortion scripts in real-time should be a high priority for content moderators.

4. **TikTok, YouTube, and Scribd must take down the sextortion how-to guides, materials, and scripts that they are hosting.**

   TikTok, YouTube, and Scribd must moderate their platforms to remove manuals and tools that are actively used to blackmail, extort, and scam victims. Each of these platforms hosts sextortion material and scripts, garnering hundreds of thousands of views. This material has been subsequently used in countless sextortion schemes against minors.[79]

5. **Instagram and Snapchat should improve their detections of Account Takeovers and Sextortion behaviors.**

   Cybercriminals are known to use account takeovers on Snapchat and Instagram to more effectively socially engineer their targets and to evade bans. These platforms should prioritize elimination of illegally acquired accounts and the creation of robust security measures to prevent further account takeovers. For example, both platforms can improve detections by tracking significant upticks in account activity after account details are altered (indicative of an account takeover). They should also detect significant upticks in account activity after a first-time login from either a VPN or an elevated-risk geographical location. Instagram, Snapchat, and other platforms should improve coordination within established organizations, such as the Tech Coalition, to share indicators of sextortion, IP addresses, usernames, and other intelligence.

6. **Wizz, and its Paris-based parent company Voodoo, must take immediate action to secure the platform from endemic sextortion.**

   Sextortion on Wizz is pervasive and dangerous. The app's design, seemingly akin to a Tinder-like interface for minors, has fostered an environment ripe for the rampant spread of sextortion.[80] The absence of robust security protocols to thwart

[78] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[79] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[80] https://www.reddit.com/r/Wizz_app/comments/15bt3v1/have_you_been_blackmailed_over_nudes_on_wizz/

the creation of new sextortion accounts, coupled with the platform's inability to effectively identify such schemes or adequately moderate existing sextortion-linked profiles, creates an inherently risky environment for minors.[81] The growth of Wizz presents significant challenges to controlling the propagation of sextortion schemes, necessitating urgent action to safeguard users, especially minors.[82]

7. **The App Store and Google Play Store should enforce their store policies with regards to Wizz, as it remains a pervasive child safety risk beyond sextortion.**

The App Store and Google Play Store should monitor and take action on app reviews of children being sexually exploited on Wizz and other apps. Dozens of parents and children post reviews of their experience being sextorted on Wizz in the App Store[83] and Google Play Store.[84]

Beyond the pervasive sextortion problem on Wizz, the app appears to be egregiously non-compliant with App Store and Google Play policies. For example, Apple's App Store policy 2.5.18 states that "Ads displayed in an app must be appropriate for the app's age rating."[85] Similarly, Google Play's policy states "The ads [...] shown within your app must be appropriate for the content rating of your app."[86] Despite this, there have been scores of complaints from parents and kids that Wizz serves pornographic advertisements to minors on their platform—including "age-verified" profiles confirmed belonging to minors.[87] [88] [89] [90]

[81] https://www.bark.us/app-reviews/apps/wizz-app-review/
[82] https://www.nbcnews.com/tech/social-media/friend-finding-app-offered-safe-space-teens-sextortion-soon-followed-rcna91172
[83] https://apps.apple.com/us/app/wizz-app-chat-now/id1452906710
[84] https://play.google.com/store/apps/details?id=info.wizzapp&hl=en_US&gl=US
[85] https://developer.apple.com/app-store/review/guidelines
[86] https://support.google.com/googleplay/android-developer/answer/9857753
[87] https://www.reddit.com/r/Wizz_app/comments/14sicj3/wizz_got_the_most_insane_ads_i_ever_seen/
[88] https://www.reddit.com/r/Wizz_app/comments/18jxlvf/how_is_this_allowed_bro/
[89] https://www.reddit.com/r/Wizz_app/comments/150eshw/wizz_got_the_most_insane_ads_i_ever_seen_part_2/
[90] https://www.reddit.com/r/Wizz_app/comments/176fosx/this_not_crazy/

Recommendations to Parents & Families

Open Conversations: Have conversations about online risks with your children. Continue to counsel children to not share intimate photos with anyone, especially a stranger online. But most importantly, let your children know that when it does happen, they are safe coming to you for help.

Understand Instagram's Risks: Inform your children that on Instagram, there are criminal accounts pretending to be youth. These accounts often initiate intimate conversations in an attempt to entrap sextortion victims. Understand that the moment someone accepts an unknown person's Follow request, their entire Followers & Following lists are exposed, giving criminals the leverage they need to conduct a highly effective extortion scam.

Snapchat Misconceptions: Have informed conversations about Snapchat. Make children aware that photos can be saved and screenshotted. Combat the belief that photos sent on Snapchat disappear, which can create a false sense of security. Additionally, emphasize that pre-recorded "catfish" videos can be sent to appear as a "live photo" or "live video" from criminals, bypassing yet another product safety feature.

Wizz: Schools,[91] parent advocacy networks,[92] law enforcement,[93] and watchdog organizations[94] have strongly advised children to steer clear of the Wizz app. Parents should emphasize its dangers and make sure they understand the risks associated with using it.

Community Involvement: Raise awareness in your community, schools, sports teams, and youth groups about the dangers of sextortion and ways to prevent it. Work on destigmatizing conversations about sextortion. Encourage openness in discussing experiences and the scope of the problem, which can be a significant step towards undermining the tactics of criminals.

Educational Resources: Review publications from organizations like NCMEC and the FBI, or the equivalent organizations in your country, for detailed guidance from law enforcement.

[91] https://roughwoodprimary.org/2023/03/14/online-safety-wizz-app/
[92] https://www.commonsensemedia.org/app-reviews/wizz-make-new-friends
[93] https://www.timescall.com/2023/08/08/longmont-teen-becomes-victim-of-sextortion-case-involving-wizz-app/
[94] https://www.bark.us/app-reviews/apps/wizz-app-review/

If you become a victim of sextortion...

Block the criminal. Report the account. Do not pay. Do not continue contact. Save any evidence for law enforcement. Deactivate the accounts where criminals contact you. Speak with a parent, friend, or trusted adult; they will support you through this process.

Report the incident to authorities. In the United States, report to the FBI's cybercrime portal IC3.gov and if you're a minor, also report to NCMEC's Cypertipline at report.cybertip.org. You can also call the FBI Field Office 24/7 Tipline nearest you or the NCMEC 24/7 hotline at 800–843–5678.

Several services have been introduced in partnership with NCMEC and Meta to prevent non-consensual imagery from being shared on social media. This includes StopNCII.org (for anyone) and TakeItDown.NCMEC.org (for minors), which hash the photos and block future uploads of the blacklisted photos to social media sites.

Be aware of post-victimization recovery scams and for-profit entities taking advantage of sextortion victims. There are legitimate and illegitimate businesses targeting sextortion victims.[95]

The FBI warns victims of for-profit firms exploiting sextortion victims by charging high fees for assistance. Unlike law enforcement and non-profit agencies, these companies use deceptive tactics like threats and manipulation to coerce payments. Some services offered, such as cease and desist orders, may provide emotional relief but lack legal enforceability.[96] Additionally, these companies discourage victims from reporting sextortion to law enforcement in their advertisements targeted at victims claiming "the police can't help you."[97]

Furthermore, NCRI has observed coordinated inauthentic activity of accounts promoting illegitimate "sextortion recovery services." These accounts often portray themselves as hackers, cybersecurity experts, or reputation management firms, but are simply another scam fuelling account takeovers.[98]

[95] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[96] https://www.ic3.gov/Media/Y2023/PSA230407
[97] https://adstransparency.google.com/advertiser/AR00520246364907503617?origin=ata&region=US
[98] https://www.cbc.ca/news/canada/british-columbia/sextortion-recovery-scams-1.6774652

SUPERIOR COURT CIVIL CASE INFORMATION STATEMENT (CIS)

COUNTY: **N** K **S** CIVIL ACTION NUMBER: **N25C-12-250 CLS**

CAPTION: ROSALIND "ROS" DOWEY, Individually and as Administrator of the Estate of M.D., MARK DOWEY, Individually and as Administrator of the Estate of M.D., et al Plaintiffs, v. META PLATFORMS, INC. and INSTAGRAM, LLC, Defendants.	CIVIL CASE CODE: ***CPRL*** CIVIL CASE TYPE: ***Personal Injury*** MANDATORY NON-BINDING ARBITRATION (MNA): **NO** NAME AND STATUS OF PARTY FILING DOCUMENT: ***See Caption, Plaintiffs*** DOCUMENT TYPE: (E.G., COMPLAINT; ANSWER WITH COUNTERCLAIM) ***Amended Complaint*** JURY DEMAND **X** YES _____NO
ATTORNEY NAME(S): ***Joseph J. Rhoades and Stephen T. Morrow*** FIRM NAME: ***Rhoades & Morrow LLC*** ADDRESS: ***Rhoades & Morrow LLC*** ***1225 King Street, Suite 1200*** ***Wilmington, Delaware 19801*** TELEPHONE NUMBER: ***302-427-9500*** FAX NUMBER: ***302-427-9509*** E-MAIL ADDRESS: joe.rhoades@rhoadeslegal.com stephen.morrow@rhoadeslegal.com	IDENTIFY ANY RELATED CASES NOW PENDING IN THE SUPERIOR COURT BY CAPTION AND CIVIL ACTION NUMBER INCLUDING JUDGE'S INITIALS EXPLAIN THE RELATIONSHIP(S): **This Amended Complaint adds additional parties and allegations to the original Complaint.** OTHER UNUSUAL ISSUES THAT AFFECT CASE MANAGEMENT: (IF ADDITIONAL SPACE IS NEEDED, PLEASE ATTACHPAGES)

THE PROTHONOTARY WILL NOT PROCESS THE COMPLAINT, ANSWER OR FIRST RESPONSIVE PLEADING IN THIS MATTER FOR SERVICE UNTIL THE CASE INFORMATION STATEMENT (CIS) IS FILED. THE FAILURE TO FILE THE CIS AND TO HAVE THE PLEADING PROCESSED FOR SERVICE MAY RESULT IN THE DISMISSAL OF THE COMPLAINT OR MAY RESULT IN THE ANSWER OR FIRST RESPONSIVE PLEADING BEING STRICKEN.

IN THE SUPERIOR COURT OF THE STATE OF DELAWARE

ROSALIND "ROS" DOWEY, Individually and as Administrator of the Estate of M.D., MARK DOWEY, Individually and as Administrator of the Estate of M.D. and TRICIA MACIEJEWSKI, Individually and as Administrator of the Estate of L.M.,	:	C.A. No. N25C-12-250 CLS
	:	TRIAL BY JURY DEMANDED
Plaintiffs,	:	
v.	:	
META PLATFORMS, INC. and INSTAGRAM, LLC,	:	
Defendants.	:	

CERTIFICATE OF SERVICE

I, Stephen T. Morrow, Esquire, hereby certify on this 27h day of February, 2026 I have served a true and correct copy of the foregoing documents via electronic service, File & ServXpress, upon all counsel of record.

RHOADES & MORROW, LLC

Stephen T. Morrow
Stephen T. Morrow, Esquire