

Exhibit 139

Child Safety State of Play (9/24)

Child Exploitation

Where are we with the various policy discussions relating to children on our apps.

Policy Landscape

Our encryption announcement has created tremendous anxiety among CSAM safety stakeholders, and generated significant legislative activity across the globe centered around exceptional access and other technical requirements and/or intermediary content liability, as well as calls to break us up. Multi-national and multi-sector bodies, including the Five Eyes, the EUIF, and the WePROTECT Global Alliance, are driving a coordinated campaign against our message encryption plans, which has caught the attention of our advertising clients as well as large foundations such as the Oak Foundation and Skoll, and driven shareholder inquiries. A spike in CSAM reporting and increased dependence on online technologies during the pandemic has made this issue COVID 19 resilient. There is some risk we become isolated from the rest of industry, which could result in FB specific solutions (e.g., Apple has tried to differentiate FB e2e messaging based on social graph). Priority Countries: US, UK, Australia, India, EU and Brazil (other potential hot spots due to high incidence rates and/or active child exploitation legislation Philippines, S. Korea, Taiwan, Japan, and South Africa).

Legislative/Regulatory Action

Trends:

- **Child Safety concerns leading to expansion/conflation of illegal and harmful content regulation.** Following UK's Online Harms Paper and Germany NetzDG, Australia has proposed expanding the eSafety Commissioner's remit to enforce on expanded harms (e.g bullying & harassment) not only for children but also adults and is also extending the scope of harms from illegal to harmful content. Countries such as Brazil, the Philippines and Indonesia are all considering misinformation and child safety in the same category in recent legislations. In Pakistan child safety issues are being used to push the Citizen Online Protection Rules to curb free speech.
- **Dedicated child safety regulators being proposed.** Australia and Fiji already have an eSafety Commissioner. Legislators in Ireland, Taiwan, the Philippines, and South Korea are considering similar offices and India has proposed an eSafety Commissioner for each state.
- **Multiple reporting requirements:** India, South Korea, and Portugal are introducing legislations that will require us report CSAM directly to local authorities and not accepting NCMEC reports.
- **Competing legislation exposing safety/privacy tensions:** The ePrivacy Directive v eSafety strategy, and secrecy of communications provisions in Japan v Japan's Amended Telecommunications Broadcasting Act guidelines on SoC provisions and and secrecy of communications provisions Korea v intermediary liability law for NCII and CEI that requires collecting and sharing of more user information with local authorities/civil complainants.

Specific Bills:

- US: EARN-IT, DoJ/White House Section 230 reforms, Platform Accountability and Consumer Transparency Act, Online Freedom and Viewpoint Act, House Appropriations Bill on Labor, HHS, and Education funding, Transparency about Online Child Sexual Abuse Material Act
- UK: Cloud Act negotiations, TCN, Online Harms Bill
- AU: ongoing consultation on Online Safety Act, e-Safety Commissioner Safety by Design Principles
- Five-Eyes: Voluntary CSEA Principles

various African countries exploring the same; and in Korea where such legislation already exists they are exploring mechanisms for verifying parental consent.

Specific Bills:

- US: FTC to update COPPA rules (expected in 2020)
- UK: Age Appropriate Design Code (likely implemented in H1 2021 subject to Parliamentary approval), Online Harms Bill
- Ireland: Child Safety and Media Regulation
- Australia: eSafety Commissioner's Safety by Design principles, amendments to the Online Safety Act
- Brazil: Internet Steering Committee ("CGI") focused on ads for minors and use of minors data (e.g. Bill 1746/2015)
- Germany: Federal and Interstate Youth Law (likely to come into effect in H2 2020; proposes browser-level age verification for German citizens)
- South Africa: Protection of Personal Information Act 4 of 2013 (July 1, 2021)
- Philippines: Safer Internet Bill (parental consent for U18s)
- India: Personal Data Protection Bill, 2019 (requires age verification and parental consent)
- SSA: Zimbabwe's Cyber crimes bill (parental consent and robust age verification), South Africa Films and classification amendment act 2020 (registration, self classification, age verification for pornographic sites), Kenya Data Protection Act 2019 (age verification for under 18's on social media platforms)
- Indonesia and Philippines: Draft bills w/r/t age-verification to ensure minors not exposed to "inappropriate/immoral content"
- South Korea and Japan: Proposals requiring we verify age through mobile phone numbers
- Colombia/Peru/Paraguay/CENAM: routine bills on mandating blocking content for kids (video games, social media, educational, etc)

Where we think we are most vulnerable and need to step up our efforts.

Immediate Product Vulnerabilities

- We lack a U13 classifier, insufficient means to detect and remove u13s at scale
- We also have deprioritized u13 enforcement because COPPA compliance is at risk when we sit on knowledge of u13, incentivizes not knowing
- Age prediction models are not that accurate, reducing the efficacy of classifiers like the grooming classifier and requiring more reliance on human review
- Age prediction models are not globally operational; as a result, integrity measures that leverage age are inconsistent and unreliable, including child safety protections
- Age prediction models are not globally resilient, they tend to perform better in Western markets and worse in emerging markets
- Age models do not work as well on IG; as a result, we have no ability to more granularly gate minors out from age-related experiences on Instagram.
- As a result of all of the above, age-gating doesn't work as well as it should yet we offer age-gated products like Watch Together, FB Dating,... and we have minors who appear as young as 12 years old.
- Lack of u18 checkpoint: Risk having u18 users on 18+ products like FB Dating, Marketplace, Mentorship, or as under-age parents on Messenger Kids
- Age verification: We remain reactive on age verification, pushing for a device side solution, when we're getting increasing policymaker pressure to be proactive while our competitors improve their approaches