Cybersecurity and AI Law Report

The Next Saga in the End-to-End Encryption Debate: When the Cure Becomes the Crisis

Cybersecurity and AI Law Report
By Rajeev Raghavan, Matthew Ferraro, Joanna Rosen Forster and Emily Welsch
August 19, 2026

On January 31, 2024, the Senate Judiciary Committee put the CEOs of Meta, TikTok, Snap, X and Discord under oath at a hearing on online child sexual exploitation. A month earlier, in December 2023, the New Mexico AG filed a lawsuit against Meta alleging that Facebook, Instagram, Messenger and WhatsApp were marketed as safe while exposing children to sexual exploitation, grooming, trafficking, self-harm content and addictive design.

About two years later, in March 2026, a New Mexico jury found Meta liable for misleading consumers about the safety of its platforms and endangering children, ordering Meta to pay $375 million for violating consumer protection laws. Then, in August 2026, a New Mexico judge ordered Meta to pay an additional $567 million to address youth mental health and imposed sweeping, court-supervised reforms to Facebook and Instagram. Among other measures, the court required Meta to eliminate push notifications for users under 18 during nighttime and school hours, limit minors' use of the platforms to 90 hours per month and maintain for five years its previously announced cessation of end-to-end encryption (E2EE) on Instagram.

Meta's adoption of E2EE played a significant role in both the trial and during the 2024 Senate hearing. The Senate Judiciary Committee had scheduled another hearing for earlier in the summer of 2026 – postponed to an unannounced future date – bluntly framed, according to news sources, as whether social media is having its "Big Tobacco moment." That is the backdrop for the next platform-design fight: not whether end-to-end encryption is valuable, but whether social networks that serve minors can still defend it as a default.

This article examines how the E2EE debate has evolved over time and how congressional interest and litigation, including the New Mexico verdict, inform practical platform considerations for use of E2EE.

The New Mexico Verdict

The New Mexico case against Meta turned encryption from a technical feature into courtroom evidence.

Allegations of Unkept Safety Promises

New Mexico AG Raúl Torrez sued Meta under the state's consumer protection laws, alleging that Meta made deceptive statements and omissions, and engaged in deceptive product design and business practices. Encryption entered the case as part of that product-design story. The complaint cited criticism from the Canadian Centre for Child Protection that Meta's reporting tools were inadequate. The AG alleged that WhatsApp's E2EE limited Meta's ability to act on reports, and that Messenger's "Secret Conversations" created similar barriers to monitoring. The

point was that in a teen-heavy social ecosystem where minors can be discovered, contacted, groomed and exploited, E2EE can make safety promises harder to keep.

Evidence of E2EE Harms for Minors

The trial evidence made that argument sharper. Reuters reported that internal Meta materials showed executives warning that encrypting Facebook and Instagram messaging could dramatically reduce child exploitation reports to the National Center for Missing & Exploited Children (NCMEC) and could impede referrals involving child exploitation, sextortion, terrorism and school shooting threats.

Evidence of internal communications dating to 2019 demonstrated that not only was Meta aware of human trafficking and grooming occurring on Instagram and Facebook, but also that it knew these issues would be exacerbated if E2EE was implemented. Trial testimony from NCMEC and an agent with the New Mexico DOJ confirmed that the suspicions came true – the number of reports to NCMEC decreased significantly after Meta implemented E2EE.

Meta disputed the state's framing and said it built safety features before incorporating broader E2EE, including easier user reporting tools. But the state's narrative was simple and potent. Meta knew visibility mattered, then made itself less able to see.

Order to Keep E2EE Cessation in Place on Instagram

The New Mexico verdict is not an anti-encryption edict in disguise; it is riskier for platforms than that. It shows how encryption can become evidence of knowledge, design choice and misrepresentation. After the verdict, New Mexico's requested injunctive relief included eliminating E2EE for users under 18, so Meta would no longer "blind" itself and law enforcement. While the court did not adopt the state's request for a prohibition on E2EE – because Meta had "already ceased offering E2EE on its Instagram platform" – it did order the cessation remain in place for five years. In contrast, the court did not order the elimination of E2EE on Facebook, because Facebook has few adolescent users in New Mexico.

Efforts to Enjoin E2EE in Other States

New Mexico's success in enjoining E2EE for several years on Instagram may spur further efforts in other states, which are already in the offing. In 2024, Nevada AG Aaron Ford sought an emergency order to stop Meta from providing E2EE to minors in Nevada, arguing that E2EE protects predators and impedes law enforcement efforts to protect children. Privacy advocates attacked the move as a dangerous assault on encryption, but the litigation theory was clear – when minors are involved, state AGs will treat platform blindness as a child safety defect, not merely a privacy feature.

The Momentum Was Growing Before New Mexico

The January 2024 Senate Judiciary Committee hearing gave political oxygen to the argument that E2EE can undermine child safety efforts. At the January 2024 hearing, Discord CEO Jason Citron used his opening statement to draw a line between Discord and platforms moving toward E2EE messaging. Stating that Discord did not believe it could "fulfill [its] safety obligations if the text messages of teens are fully encrypted," the CEO noted that E2EE would "block [its] ability to investigate a serious situation and when appropriate report to law enforcement."

At the hearing, Senator Mike Lee (R-UT) said he strongly supported privacy and E2EE, but noted that "a great deal of grooming and sharing" of child sexual abuse material (CSAM) happens on E2EE systems. He then pressed Meta CEO Mark Zuckerberg on whether minors could use Meta products with E2EE. Zuckerberg acknowledged that users under 18 could use WhatsApp's E2EE messaging service. Regarding Discord, Citron stated that the company did not use E2EE for text messages because it believed "that it's very important to be able to respond to [] law enforcement requests." Senator Lee's line of questioning now frames the broader debate – that encryption can be useful, but it can be harmful on sites where children are being groomed and exploited.

Since around 2019, NCMEC has been even more direct. It has warned that E2EE prevents platforms from detecting illegal activity, including online demand for CSAM and that, without exceptions for child exploitation detection, "millions of incidents of abuse will remain hidden." According to NCMEC, its CyberTipline access is sometimes the only way law enforcement can rescue a child or identify an offender.

CyberTipline reporting – mandated by federal law – is directly affected by E2EE. During testimony before the House Energy and Commerce Committee in March 2025, NCMEC's chief legal officer, Yiota Souras, noted that online platforms had reported seven million fewer incidents to the CyberTipline in 2024 than they had in 2023. Souras attributed the drop principally to Meta's decision to implement default E2EE on Facebook Messenger.

The FBI has made a similar argument. In 2022 Senate testimony, FBI Director Christopher Wray explained that E2EE can prevent law enforcement, even with valid legal process, from finding victims and evidence. He specifically warned that child exploitation tips from platforms depend on the providers being able to detect and report abuse on their services – and that they cannot do that when the relevant environments have E2EE.

Calculating the Appropriate Approach to E2EE

On March 17, 2026, Meta announced that Instagram would discontinue optional E2EE direct messages (DMs) – just days before the New Mexico trial reached its close. Pointing to low adoption, Meta directed users who wanted E2EE messaging toward WhatsApp. But the timing told its own story: encrypted Instagram DMs carried limited product upside and major courtroom downside.

In the next chapter of the E2EE debate, platforms may need to reassess the role of this technology in product decisions in light of growing litigation, regulatory scrutiny and child-safety concerns along the following lines.

Consider Segmentation

The smart platform response may not have to be "privacy is over." Instead, a platform could turn toward segmentation. Social discovery platforms, such as Instagram, where minors, creators, strangers, recommendations, media and messaging collide, present potentially different risk profiles than a one-to-one messaging application, such as Signal or iMessage.

As platforms look to adapt, the future may be selective E2EE – available in standalone messaging but unavailable in environments where minors could communicate with strangers. With jurisdictions around the world starting to require reliable age verification measures, platforms may be better positioned to tailor features and safeguards to different age groups.

Look at Enhancing Real-Time Reporting Infrastructure

Moving away from E2EE could create a new set of legal problems. Seeing may create duties. As previously noted, in the United States, platforms that become aware of apparent child sexual exploitation must report to NCMEC. When a platform can inspect more content, it may need to increase its real-time detection and reporting infrastructure.

Enhancements could involve incorporating technologies to detect CSAM on the platform, including CSAM hash matching, unknown-CSAM classifiers, and grooming and sextortion detection. With stronger detection, platforms also may need to build out internal processes to better action child sexual exploitation reports, such as escalation queues, preservation workflows, trained human review and reliable user-reporting paths.

Get Ahead of Deepfakes

Deepfakes – AI-generated imagery and videos – raise the stakes. NCMEC reported 1.5 million 2025 CyberTipline reports with a generative AI nexus, including AI-generated CSAM and manipulation of known CSAM. Congress also responded to this growing trend with the TAKE IT DOWN Act (Act), signed into law in May 2025. The Act, which went into effect in May 2026, targets nonconsensual intimate imagery, including AI deepfakes, and requires covered platforms to remove qualifying material within 48 hours after valid notice. The Act does not exempt E2EE services, leaving it up to the platforms to determine how to remove illegal content that they cannot view or access.

Plan to Address Law Enforcement Requests

Companies should not underestimate the wave of legal process from law enforcement. When a platform has E2EE, prosecutors and law enforcement know it. They may still send preservation demands, subscriber subpoenas, IP requests or metadata process, but they often do not waste time demanding message content they know the platform cannot decrypt. Once a platform can access message content, law enforcement is far more likely to seek communications that were previously unavailable.

The flood of legal process will include subpoenas, warrants, emergency requests, CyberTipline follow-ups, regulator subpoenas, civil discovery and even wiretaps. The Stored Communications Act gives law enforcement mechanisms to compel the production of stored communications, and records and federal wiretap law can require platforms to furnish technical assistance necessary to accomplish lawful interception.

National security demands could rise, too. Director Wray's public testimony also tied E2EE to terrorism and other grave threats. For U.S. platforms, foreign evidence demands likewise could increase. Once platforms can access and produce more unencrypted content, Mutual Legal Assistance Treaty requests, CLOUD Act requests and other jurisdictional demands may become part of the new operational reality.

Platforms that built legal-response teams relying on the inherent limitations of E2EE may need to suddenly support real-time interception, minimization, auditability and round-the-clock escalation. Doing so could involve developing or revising company policies regarding law enforcement requests, retraining or hiring additional staff, and even leveraging AI to help deal with the influx.

Balance Privacy Obligations

Privacy law is the counterweight to E2EE reform – especially outside the U.S. The European Union ended one chapter of its own debate regarding how to handle E2EE and CSAM when, in March 2026, the E.U. Parliament rejected a proposed expansion of the controversial "Chat Control" plan. The Chat Control plan would have allowed platforms to scan encrypted messages for CSAM (with one failed proposal even making it a requirement to do so). The European Data Protection Board highlighted the importance of encryption as a privacy tool in its 2022 recommendations about the plan, noting the delicate balance between privacy concerns and protecting children online.

In the U.S., there is no single federal comprehensive privacy law or centralized regulating body, but there is a long legal tradition of a right to privacy and a patchwork of statutes codifying the rights of consumers to make decisions about their data. For example, the CCPA gives California consumers rights to know, delete and control certain uses of PI. For regulated businesses, the CCPA mandates transparency about what data they collect and why, and requires entities to build out features for consumers to exercise those rights in a way that will be honored. A platform that abandons encryption but continues to market messages as private could be inviting a different lawsuit, including potentially for misleading or deceptive claims.

The Road Ahead

Platforms may now face a difficult policy balance. They need to monitor for CSAM, support abuse reporting, scan for known abuse material, detect grooming and sextortion, and respond quickly to deepfake and takedown demands. But they may also need to account for privacy concerns, such as data minimization, access controls, retention limits, audit logs, transparency and privacy-by-design. "We encrypted it, so we cannot help" may become less tenable; "we scan everything, trust us" may not be a solution either.

The New Mexico verdict was not the death knell for E2EE. It foreclosed the easy argument that encryption is always the safest default, regardless of product context. The new rule could be sharper. If a company connects children with strangers, recommends accounts, hosts media, enables DMs and promises safety, E2EE may no longer be a cure-all but a source of risk. It may just be one part of the overall safety design – and juries, AGs, Congress, NCMEC and law enforcement are now treating it that way. When representatives for major technology platforms once again take center stage on Capitol Hill, we will see how the conversation surrounding E2EE and child online protection continues to evolve.

Rajeev Raghavan is a partner in Crowell & Moring's privacy and cybersecurity group and a former special counsel to the Director of the Federal Bureau of Investigation and federal prosecutor. He advises clients on high-stakes cybersecurity and privacy incidents, government investigations and enforcement actions, sensitive national security matters, and litigation.

Matthew Ferraro is a partner in Crowell & Moring's privacy and cybersecurity group and a former senior counselor for cybersecurity and emerging technology to the Secretary of Homeland Security. He advises clients on complex regulatory matters at the intersection of advanced technology, national security and crisis management.

Joanna Rosen Forster is a partner in Crowell & Moring's litigation group and a former general counsel of a global ecommerce platform and former deputy AG in the Corporate Fraud Section

of the California DOJ. She advises clients on complex commercial disputes and regulatory matters related to emerging technologies and speech online, including high-stakes litigation, class actions, and government investigations.

Emily Welsch is an associate at Crowell & Moring, working within the litigation and privacy and cybersecurity groups. She represents clients in complex litigation and regulatory matters, including advising on technology-related