BREF

CHRISTOPHER M. PETERSON, ESQ. (13932)
AMERICAN CIVIL LIBERTIES
UNION OF NEVADA
4362 W. Cheyenne Ave.
North Las Vegas, NV 89032
Telephone: (702) 366-1226
Facsimile: (725) 210-6328
Email: peterson@aclunv.org
Attorney for Amici Curiae

JENNIFER STISA GRANICK, ESQ.*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
425 California St., 7th Fl.
San Francisco, CA 94104
Telephone: 415-343-0758
Email: jgranick@aclu.org
**Pro hac vice* forthcoming

DISTRICT COURT

CLARK COUNTY, NEVADA

STATE OF NEVADA,

Plaintiff,

vs.

META PLATFORMS, INC. f/k/a FACEBOOK, INC.,

Defendant.

Case No. A-24-886110B

Dept. No. XXXI

Hearing Not Requested

Brief of *Amici Curiae* American Civil Liberties Union, American Civil Liberties Union of Nevada, Electronic Frontier Foundation, Riana Pfefferkorn, Access Now, Center for Democracy and Technology, Fight for the Future, Internet Society, Mozilla Corporation, and Signal Messenger LLC, In Support of Defendant Meta Platforms.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENTS OF INTEREST[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization dedicated to defending the civil liberties and civil rights guaranteed by the federal and state Constitutions, and the ACLU of Nevada is the ACLU's Nevada affiliate.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported digital civil liberties organization representing the interests of technology users in court cases and broader policy debates surrounding the application of law to technology.

Riana Pfefferkorn is a Research Scholar at the Stanford Internet Observatory, where her research focuses on encryption policy, online privacy, cybersecurity, and online trust and safety, particularly child safety. She appears in her personal capacity only and does not represent the Stanford Internet Observatory, the Stanford Cyber Policy Center, or Stanford University.

Access Now is an international non-profit organization working to strengthen the digital rights of people and communities at risk. Access Now engages courts in the United States and abroad, advocating for privacy, freedom of

[1] Pursuant to Nev. R. App. P. 29, all parties consented to the filing of this brief. See EXHIBIT A for consent from Plaintiff State of Nevada. See Exhibit B for consent from Defendant Meta Platforms.

expression, and civic space online.

The Center for Democracy & Technology ("CDT") is a non-profit organization that represents the public's interest in an open, decentralized Internet. We work to protect constitutional and democratic values in the digital age. CDT supports encryption because it is essential to communications security, privacy, and free expression.

Fight For the Future is composed of artists, engineers, activists, and technologists who recognize that tech policy issues have a disproportionate impact on communities of color, low-income people, religious minorities, political dissidents, LGBTQ people, and others who face systemic oppression.

The Internet Society is a global charity and non-profit organization with the vision that the Internet is for everyone. Its primary objective is to coordinate and collaborate on issues related to improving the Internet, including standards, applications, and policies, and defend against actions that threaten the way that the Internet operates.

Mozilla Corporation is a global, mission-driven organization that creates open source products like its web browser Firefox. It is guided by the Mozilla Manifesto, a set of principles that recognizes that individuals' security and privacy on the Internet are fundamental. Mozilla Corporation is a wholly-owned subsidiary of the Mozilla Foundation, a 501(c)(3) non-profit. Mozilla Corporation issues no

stock, and no publicly held corporation owns a ten-percent or greater interest in it.

Signal Messenger LLC is an independent non-profit whose widely used messenger is the gold standard for accessible end-to-end encrypted messaging. Our Signal Protocol also underpins secure communication for billions of people, safeguarding the fundamental human rights of privacy and freedom of expression.

INTRODUCTION

End-to-end encryption ("E2EE") ensures the privacy and confidentiality of messages exchanged between users by encrypting the content of the messages when sent, then decrypting them when received, making them unreadable while in transit by anyone other than the sender and intended recipient. This means that even if someone intercepts the messages—be they the service provider, a criminal, domestic abuser, foreign despot, or law enforcement—they will be unable to decipher the message. Nothing about end-to-end encryption prevents law enforcement from accessing the message in readable form from either the recipient or the sender. Nor does end-to-end encryption on Messenger prevent Meta from disclosing non-content "metadata" about conversations to police with proper legal authorization.

Encryption has played a crucial role in protecting private communications, especially in political and military contexts, going back to Caesar and through the

Founding of the United States.[2] With the rise of the Internet, it has become vitally important to ordinary people as well. That is because the Internet originally did not widely support secure communication, making most private communications readily subject to eavesdropping, posing a privacy and security risk unlike any other in history. Encryption is the best means we have for protecting these communications, and these protections are as important for children as they are for adults.

U.S. law and policy have long recognized the value of encryption. It has been the subject of longstanding debate and discussion among computer scientists, national security officials, law enforcement, experts on business, innovation, and commerce, diplomats, spy agencies, human rights advocates, and civil libertarians. While opinions about how and where encryption should be used have fluctuated over time, the consistent policy of the United States has been to permit companies to use encryption to protect users and their data.[3] U.S. laws balance our security

---

[2] Seth Schoen & Jamie Williams, *Crypto is For Everyone—and American History Proves It*, Gizmodo (Nov. 1, 2015), https://gizmodo.com/crypto-is-for-everyone-and-american-history-proves-it-1739874890 (reprintedhttps://gizmodo.com/crypto-is-for-everyone-and-american-history-proves-it-1739874890 (reprinted from EFF.org); Joseph A. Mussulman, *Jefferson-Lewis Cryptology: Jefferson's ciphers*, Lewis & Clark, https://lewis-clark.org/the-trail/eastern-beginnings/jefferson-lewis-cryptology/#Sub1.

[3] In choosing to end-to-end encrypt users' communications such that it cannot produce them in decrypted form to law enforcement, Meta is doing just what Congress has permitted it to do under statutes such as the Communications

and privacy with the needs of law enforcement by giving our government the authority to search communications that are available, while creating no obligation for companies to deny people access to tools and services that provide them protection. Affirmatively preventing companies from providing security, as the State seeks here, creates security risks from bad actors, including both criminals and government officials who would abuse their power in order to illegally access messages.[4]

The State's motion for a preliminary injunction attempts to substitute the judgment of the Attorney General's office for a national policy developed over decades of discussion with multiple stakeholders. The State paints a picture of E2EE as solely a danger to children. But the reason that E2EE has been widely adopted is that it *prevents* crime—crime affecting both children and adults. The

---

Assistance to Law Enforcement Act ("CALEA"). 47 U.S.C. § 1002 (b)(2)(A) ("information service" providers such as Meta are not required to make their subscribers' communications wiretappable by law enforcement). *In re Apple, Inc.*, 149 F. Supp. 3d 341, 354-57 (E.D.N.Y. 2016) (recognizing that Congress "prescribe[d] the private sector's duties to assist a wide variety of law enforcement investigations" and that "[n]one of those laws imposed any obligation on Apple" to undermine its encryption so that law enforcement could access data in decrypted form).

[4] The State says that it wants to ensure it can get access to Messenger communications "in response to a subpoena or warrant," Pl.'s Reply in Supp. of Motion for TRO and Prelim. Inj. at 2. The reference to "subpoena" is disturbing, since the Fourth Amendment does not allow access to communications content held by a service provider without a warrant. *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

State has many avenues for pursuing its child-safety investigations without this extraordinary order. It is especially ill-advised to upend decades-old, encryption-specific policies based on a reinterpretation of a broad, general purpose law such as the Nevada Unfair and Deceptive Trade Practices Act, N.R.S. 598.0903-598.0947.

While the Attorney General may disagree, the assertion that E2EE is good for children is a mainstream point of view and not properly classified as "deceptive" (Mot. at 16-17). Millions of children have long used E2EE platforms such as WhatsApp and iMessage. It can hardly be "unconscionable" for Meta to upgrade its product to meet the security and privacy standards that other exceedingly popular products—ones the Attorney General has not challenged—have offered to the public for years.

The motion for a preliminary injunction that would stop Meta from providing secure communications to its users is baseless and dangerous. Meta's provision of end-to-end encryption by default to all Messenger users is not deceptive or unconscionable, meaning the State is unlikely to succeed on the merits. To the contrary, because E2EE protects consumers, its continuation will not cause irreparable harm and in fact benefits the public interest (a preliminary injunction factor the State does not discuss). *Clark Cnty. Sch. Dist. v. Buchanan*, 112 Nev. 1146, 1150, 924 P.2d 716, 719 (1996). The Court should reject the State's request.

ARGUMENT

I. The privacy and security of electronic communications on the Internet are threatened in unprecedented ways, and encryption is the most important means of protecting users, especially vulnerable ones such as children.

A. Until recently, most conversations were ephemeral and beyond the reach of police.

Society has long recognized that people thrive when we have the ability to engage in private, unmonitored conversations. Sharing confidences enables people to form friendships and intimate relationships, obtain information about sensitive matters, and construct different identities depending on the audience. We know this from our own lives, whether engaging in pillow talk, meeting a friend for a walk, or forming an invitation-only club. Important, human things happen when we can be confident that no one is listening in.

Before the Internet, these conversations were not recorded or preserved. Our words vanished into the air as they were spoken. Unless someone was eavesdropping, conversations were private, secret, and unrecoverable. Police could not access these interactions. Mail carriers did not make copies of letters and senders and recipients were free to write in code or foreign languages and to destroy the documents after they had been received.

In any other era, a claim that government may obligate us to record and preserve our conversations, just in case investigators wanted to review them later, would be laughably ridiculous. It would simply have been beyond the pale to

suggest that people could be *required* to record their conversations in a language that law enforcement could readily understand and access. Basic conversational privacy was assumed, and rightly so.

B. The ability for companies, governments, and others to surveil users on the Internet threatens privacy and security, but encryption offers a means of protecting both.

The Internet's basic design means communications and other data are exchanged and potentially stored by multiple computers. The technology we use in our daily lives creates voluminous and long-lasting records about deeply personal things. Email, texts, and chat capture our conversations with friends, family, and coworkers. Our cellphones log where we've been, where we are going, and whom we are with. Our Internet activity is a window into our most personal interests. These data troves contain people's intimate documents—love notes, tax records, business plans, health data, religious and political affiliations, personal finances, digital diaries and more.

Unless encrypted, these sensitive matters would be available to anyone tapping the cables or wires that connect Internet computers, and to any operator of those computers. Yet, encryption was not built into the bones of the Internet: it has been added over time. Some of the reasons for the continued persistence of unencrypted data are commercial, including to enable targeted advertising, and some are due to the technical limitations of the early Internet, and the difficulties of

deploying changes in a distributed system. Regardless, this confluence has affected all users' security and privacy.

The Internet's original configuration, coupled with corporations' maximalist attitude towards data collection and retention, meant law enforcement got accustomed to having easy access to this sensitive and voluminous information—again, most of which never existed before, let alone in such vast quantities. All law enforcement needs to do is serve the right kind of legal process, and years' worth of photos, messages, videos, interactions are available for the taking. *See, e.g.*, *United States v. Shipp*, 392 F. Supp. 3d 300, 305 (E.D.N.Y. 2019) (Facebook disclosed 21,471 pages of private information in response to a warrant). This circumstance has led commenters to label this era a "Golden Age for surveillance."[5]

While it may be a windfall for law enforcement, from a user standpoint, the persistence and availability of this data are a privacy and security failure. Encryption presents a way to regain the privacy we've lost to the digital age.[6] The

---

[5] Peter Swire, *The Golden Age of Surveillance*, Slate (July 15, 2015), https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html.

[6] Ryan Polk, *Congress, Don't Give Away The Keys To Our Encrypted Communications*, The Hill (Mar. 3, 2024), https://thehill.com/opinion/cybersecurity/4501374-congress-dont-give-away-the-keys-to-our-encrypted-communications/

Ninth Circuit recognized encryption's importance 25 years ago in rejecting the U.S. government's export restrictions on strong cryptography (in a case handled by *amicus* EFF). The court summarized the increased need for encryption in the digital era:

> In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. . . . Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost.

Bernstein v. Dept. of Justice, 176 F.3d 1132, 1146 (9th Cir. 1999), *rehearing en banc granted*, *op. withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

Today, encryption is increasingly being deployed to protect data (including communications) both at rest and in transit. Almost all Internet traffic is encrypted in transit between users and the websites and applications they access online. Experts estimate that between 80 and 95 percent of website traffic is encrypted.[7] Google reports that over 90 percent of its emails were encrypted during transit in 2023.[8] This technology prevents law enforcement from eavesdropping on

---

[7] Alexis Hancock, *The Last Mile of Encrypting the Web: 2023 Year in Review*, Electronic Frontier Foundation: Year in Review (Dec. 25, 2023), https://www.eff.org/deeplinks/2023/12/year-review-last-mile-encrypting-web.

[8] Email Encryption in Transit, Google Transparency Report, https://transparencyreport.google.com/safer-email/ (Input the ranges Jan. 1, 2013 to Dec. 31, 2013 in Outbound and Inbound email encryption; compare figures with

encrypted communications.

Upon arrival, Internet services store user data on their machines—"in the cloud." This stored data at rest is often encrypted, but generally with decryption keys that the platform has access to. That means that anyone with access to the keys can access, share, manipulate, or otherwise interfere with the data. In order to ensure the confidentiality and integrity of Internet-stored data, communications must instead be encrypted "end-to-end," so that only the users have access. This is the next step in securing the public's data and attempting to regain some of the communications privacy we have lost due to the digital age.

The State portrays E2EE as a new and dangerous technology. But Meta has provided E2EE as an option in Messenger since 2016.[9] The truth is that Meta's introduction of E2EE for Messenger as a default makes it late compared to its competitors—even compared to Meta's own products. The market for E2EE communications is big and growing. *Amicus* Signal's "Signal Private Messenger" is E2EE by default. Thanks to Signal's encryption protocol, WhatsApp—which,

---

the results for date ranges Jan. 1, 2023 to Dec. 31, 2023); *Opportunities TLC vs Forced TLS for SMTP*, LuxSCI Blog (Jan. 23, 2024), https://luxsci.com/blog/opportunistic-tls-forced-tls.html

[9] *Messenger Starts Testing End-to-End Encryption with Secret Conversations*, Meta (July 8, 2016), https://about.fb.com/news/2016/07/messenger-starts-testing-end-to-end-encryption-with-secret-conversations/.

like Messenger, is owned by Meta— has been E2EE by default since 2016.[10] WhatsApp users send up to 65 *billion* E2EE messages per day.[11] On Apple's iMessage, which has been E2EE since its launch in 2011,[12] the number is more than 8 billion.[13] Last summer, Google Messages, with over a billion monthly active users,[14] made messages between Android users E2EE by default.[15] Now that Facebook Messenger, with an estimated 50 billion messages per day,[16] is E2EE by

---

[10] Moxie Marlinspike, *WhatsApp's Signal Protocol Integration is Now Complete*, Signal (Apr. 5, 2016), https://signal.org/blog/whatsapp-complete/; Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, Wired (Apr. 5, 2016), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

[11] Ankush Sinha Roy, *How Does Facebook Handle The 4+ Petabyte Of Data Generated Per Day? Cambridge Analytica - Facebook Data Scandal*., Medium (Sep. 15, 2020), https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4https://medium.com/@srank2000/how-facebook-handles-the-4-petabyte-of-data-generated-per-day-ab86877956f4.

[12] Press Release, Apple, *New Version of iOS Includes Notification Center, iMessage, Newsstand, Twitter Integration Among 200 New Features* (June 6, 2011), https://www.apple.com/newsroom/2011/06/06New-Version-of-iOS-Includes-Notification-Center-iMessage-Newsstand-Twitter-Integration-Among-200-New-Features/.

[13] Ch Daniel, *iMessage Revenue and Growth Statistics (2024)*, Signhouse Blog (Dec. 29, 2023), https://www.usesignhouse.com/blog/imessage-stats/.

[14] Sanaz Ahari, *New Features To Celebrate Messages' 1 Billion RCS Users*, Google Blog (Nov. 30, 2023), https://blog.google/products/android/7-new-messages-features/.

[15] Imad Khan, *Google Messages Now Uses End-to-End Encryption by Default*, CNET (Aug. 8, 2023), https://www.cnet.com/tech/services-and-software/google-messages-now-uses-end-to-end-encryption-by-default/.

[16] Nicola Bleu, *27 Latest Facebook Messenger Statistics (2024 Edition)*, Blogging

default as well, all those messages will get a level of security and privacy long provided by comparable apps.

The State offers no explanation for its claim that Meta's Messenger poses a unique threat given the widespread availability of E2EE.

C. End-to-end encryption benefits children.

Children need strong encryption to protect them and their friends and family members from bad actors. In a recent report detailing both the risks and the benefits of encryption, two respected child protection organizations, Child Rights International Network and DefendDigitalMe, outlined some of the uses of end-to-end encryption:

> . . . encrypted channels can be used to communicate safely with the outside world and seek help where children are victims of violence, for example perpetrated by a family member. Moreover, encryption engages not only children's rights to privacy and protection from violence, but also non-discrimination, the right to life, freedom of thought, conscience and religion, the right to health, and even the protection of children affected by armed conflict.

Child Rights International Network & DefendDigitalMe, *Privacy and Protection: A Children's Rights Approach to Encryption, Child Rights* vii (2023).

While children can and do need strong encryption in order to safely communicate about harms being caused by their parents or others in the home who

---

Wizard (Jan. 1, 2024) https://bloggingwizard.com/facebook-messenger-statistics/.

might be able to eavesdrop, children also benefit from strong encryption to protect ordinary communications *with* their parents which, if intercepted, can be used to target them by criminals. While Nevada dismisses such concerns as "nebulous risks" they are real. Pl.'s Reply in Supp. of Motion for TRO and Prelim. Inj. at 6. For example, in 2015, hackers stole five million customer details from a children's technology and toy firm, including sensitive information and *unencrypted chats* between children and their parents.[17] This data gave criminals the names, ages, and addresses of millions of children.[18]

As *amicus* the Internet Society points out, "Governments are right to be thinking about the best ways to keep our children safe online. But if they succeed in banning or weakening any part of the safety net encryption offers our children online, they'll make them more vulnerable to the same criminals, predators, and other horrors we *all* want to prevent online."[19]

D. End-to-end encryption helps protect against cybersecurity risks, and the protections are best achieved when E2EE is turned on by default.

As explained above, absent encryption, networked communications are

---

[17] Lorenzo Franceschi, *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*, Vice (Nov. 27, 2015), https://www.vice.com/en/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids.

[18] Id.

[19] Natalie Campbell, *Don't Make Parents Raise Kids in a World without Encryption*, Internet Society Blog (Feb. 9, 2021), https://www.internetsociety.org/blog/2021/02/dont-make-parents-raise-kids-in-a-world-without-encryption/.

fundamentally insecure. Anyone with access to the servers that store our data or the networks that transmit it would be able to intercept or tamper with any communication. That poses a critical threat to the security of us all.

In the past few years, as networks have been exploited by criminals and foreign governments, officials have become increasingly concerned about cybersecurity weaknesses. Successful attacks on the Office of Personnel Management,[20] Sony Pictures,[21] and the private photos and other material of celebrities and others[22] have led government and industry leaders to push for stronger security, including increased use of encryption. Encrypting data is now considered a standard baseline cybersecurity measure for protecting Americans' personal information.

But the protections that strong encryption affords users (adults and children alike) are illusory if E2EE is not actually adopted. That is the case when E2EE is merely an optional setting, as it used to be in Messenger. Most people never

---

[20] Elizabeth Weise, *Second Hack At OPM May Have Been Worse Than First*, USA Today (June 12, 2015), http://www.usatoday.com/story/tech/2015/06/12/office-of-personnel-management-hack-china/71146452/.

[21] Bruce W. Bennett, *Did North Korea Hack Sony?*, The Rand Blog (Dec. 11, 2014), http://www.rand.org/blog/2014/12/did-north-korea-hack-sony-pictures-entertainment.html.

[22] Charles Riley & Jose Pagliery, *Apple To Beef Up Security Measures After Nude Photo Leak*, CNN (Sept. 4, 2014), http://money.cnn.com/2014/09/04/technology/security/apple-celebrity-photos/index.html.

change the default settings that come pre-set in their apps and devices.[23] That is, users are much less likely to use a setting if they must opt-in to it rather than opt-out from it. Even when users do change default privacy settings, the outcome does not always match expectations.[24] Defaulting to a more privacy-protective setting is thus a more reliable way for apps to respect user privacy than making users jump through hoops to protect themselves.

Previously, Messenger users had to know the E2EE option existed and seek it out. And since it was not a blanket setting, they had to remember to turn it on for each conversation they wished to make E2EE.[25] And if any party to the conversation did not have access to the E2EE feature, the option to enable it for the conversation would not be available even to those with access to the feature. Now that E2EE is available and the default for everyone, Messenger users don't have to

---

[23] See generally Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspective from Law, Computer Science and Behavioral Economics*, 82 Notre Dame L. Rev. 583 (2006).

[24] Yabing Liu *et al.*, *Analyzing Facebook Privacy Settings: User Expectations vs. Reality*, IMC '11: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference 61, 65 (Nov. 2011) (in a user research study about Facebook privacy settings, "it is known that users do not always adjust default settings," and "even … where the user has explicitly adjusted privacy settings" when uploading photos to Facebook, the results "still do not match the users' expectations the majority of the time").

[25] Alina Bradford, *How to Enable End-to-End Encryption on Facebook Messenger*, CNET (Oct. 4, 2016), https://www.cnet.com/tech/mobile/secret-conversation-how-to-enable-messengers-end-to-end-encryption/ ("You will need to turn on this option for every conversation or else you won't get the encryption protection.").

do anything, pay attention to confusing indicators, nor even know what encryption is (as surely few children do), for the confidentiality, integrity, and security of their online conversations to be protected.

The importance of defaults is why California recently enacted child safety legislation (modeled on a similar law in the U.K.) requiring online services likely to be used by children to set child users' default privacy settings to those that "offer a high level of privacy" (absent a compelling reason to do otherwise). California Age-Appropriate Design Code Act, CAL. CIV. CODE § 1798.99.31(a)(6) (2024). California's law is deeply flawed and even unconstitutional in other respects, as *amici* EFF and ACLU recently explained to the Ninth Circuit in a pending constitutional challenge to the law.[26] But it got this much right: while everyone deserves privacy online, strong default privacy settings are especially important for young users. Online service providers like Meta (long notorious for its confusing privacy settings[27]) should not be forced to put the burden on children

---

[26] Mario Trujillo, *EFF to Court: Strike Down Age Estimation in California But Not Consumer Privacy*, Electronic Frontier Foundation (Feb. 14, 2024), https://www.eff.org/deeplinks/2024/02/eff-court-strike-down-age-estimation-california-not-consumer-privacy; Press Release, American Civil Liberties Union, *ACLU, ACLU of Northern California Urge Court to Continue to Block Unconstitutional Restriction on Online Publication, Recognize Importance of Consumer Privacy Laws* (Feb. 14, 2024), https://www.aclu.org/press-releases/aclu-aclu-of-northern-california-urge-court-to-continue-to-block-unconstitutional-restriction-on-online-publication-recognize-importance-of-consumer-privacy-laws.

[27] Kevin Bankston, *Facebook's New Privacy Changes: The Good, The Bad, and*

to figure out how to protect themselves against privacy harms; rather, providers should protect children's privacy by default in the first place.

E. Federal and state regulators agree that the widespread use of encryption is good for society, and not dangerous.

Many federal agencies have long favored strong encryption. The Federal Trade Commission ("FTC") considers poor data security practices, including with respect to encryption, both unfair and deceptive. As early as 2005, the agency cited businesses' failure to encrypt consumer data (in transit and at rest) as one of the factors that made their data security practices unfair.[28] The FTC obtained a settlement against Zoom Video Communications, Inc. for telling its customers that its product was end-to-end encrypted when actually the company maintained the keys.[29] The FTC's "Start with Security" guidebook, which synthesizes lessons

---

The Ugly, Electronic Frontier Foundation (Dec. 9, 2009), https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-uglyhttps://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly ("The social networking site has rightly been criticized for its confusing privacy settings, most notably in a must-read report by the Canadian Privacy Commissioner issued in July [2009] and most recently by a Norwegian consumer protection agency.").

[28] Press Release, Fed. Trade Comm'n, *BJ's Wholesale Club Settles FTC Charges* Fed. Trade Comm'n (June 16, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-chargeshttps://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; Press Release, Fed. Trade Comm'n, *DSW Inc. Settles FTC Charges* (Dec. 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges.

[29] Press Release, Fed. Trade Comm'n, *FTC Requires Zoom to Enhance its Security*

from its data security enforcement actions, tells businesses to "[u]se strong cryptography to secure confidential material during storage and transmission … [and] configure it properly."[30] Similarly, the Government Accountability Office, with agreement from the Federal Communications Commission, Department of Homeland Security, and National Institute of Standards and Technology, recommended in 2012 that device and network providers offer strong encryption to increase security.[31]

Encryption-related and other improvements to Meta's privacy and security

---

Practices as Part of Settlement (Nov. 9, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlementhttps://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement. *See also F.T.C. v. Wyndham Worldwide Corp*., 799 F.3d 236, 241, 256 (3d Cir. 2015) (Wyndham claimed to use 128-bit encryption, but "did not use *any* encryption for certain customer files").

[30] Fed. Trade Comm'n, *Start with Security: A Guide for Business: Lessons Learned from FTC Cases* 7-8 (2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

[31] U.S. Gov't Accountability Off., GAO-12-757, *Information Security: Better Implementation of Controls for Mobile Devices* 22 (2012), http://www.gao.gov/assets/650/648519.pdfhttp://www.gao.gov/assets/650/648519.pdf ("Mobile device manufacturers and wireless carriers can implement technical features, such as enabling passwords and encryption to limit or prevent attacks."). In a separate report, the GAO specifically noted the failure of the Census Bureau to take full advantage of strong encryption in devices used by employees. U.S. Gov't Accountability Off., GAO-13-63, *Information Security: Actions Needed by Census Bureau to Address Weaknesses*, (2013), applewebdata://bf1cd7d5-8307-4251-b966-525201e4c696/"hthttp://www.gao.gov/assets/660/651448.pdf.

practices have been a longstanding objective of regulators such as the FTC. In 2012, Meta agreed to a consent order with the FTC requiring the company to establish and maintain a "comprehensive privacy program."[32] Following the Cambridge Analytica incident, which prompted investigations by multiple state attorneys general,[33] the FTC modified the 2012 order to require major reforms to Meta's privacy practices.[34] That modified order reflects the agency's emphasis on security and encryption, and it specifically highlighted the need for encryption of

---

[32] Press Release, Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers By Failing to Keep Privacy Promises* (Nov. 29, 2011), https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises; *In the Matter of Facebook, Inc.* 5, No. C-4365, 2012 WL 3518628 (F.T.C) (July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[33] *See* Makena Kelly, *Facebook isn't complying with privacy probe, California attorney general says*, The Verge (Nov. 6, 2019), https://www.theverge.com/2019/11/6/20951936/facebook-cambridge-analytica-investigation-california-court-order-documents; *see also* Shannon Liao, *Facebook is being investigated by New York and Massachusetts attorneys general over Cambridge Analytica scandal*, The Verge (Mar. 20, 2018), https://www.theverge.com/2018/3/20/17144432/facebook-investigation-new-york-massachusetts-attorney-generals-data-breach-cambridge-analytica.

[34] Press Release, Fed. Trade Comm'n, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebookhttps://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

user passwords.[35] The FTC's actions over the years send a strong message: improving Meta's privacy and security practices is of paramount importance, and robust encryption is a key component of that goal. Meta's choice to make all messages on Messenger E2EE by default is exactly the kind of user privacy and security enhancement that regulators have long urged.

Children's data is not exempt from privacy and data security requirements, as the State's brief seems to imply; to the contrary, it is an area of special concern. Just last year, the FTC issued a consent order to an "ed tech" company whose failure to adequately protect schoolchildren's (and employees') personal information led to four data breaches that exposed such sensitive information as children's birthdates, sexual orientation, and disabilities.[36] The company's use of "outdated and weak encryption" was one of the failures cited by the FTC.[37]

At the state level, multiple states impose data security requirements on

---

[35] *In the Matter of Facebook, Inc.* 7, No. C-4365, 2012 WL 3518628 (F.T.C) (July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

[36] Press Release, Fed. Trade Comm'n, *FTC Finalizes Order with Ed Tech Provider Chegg for Lax Security that Exposed Student Data* (Jan. 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-ed-tech-provider-chegg-lax-security-exposed-student-data.

[37] Press Release, Fed. Trade Comm'n, *FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers* (Oct. 31, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-brings-action-against-ed-tech-provider-chegg-careless-security-exposed-personal-data-millions.

private-sector actors to safeguard state residents' information. *E.g.*, CAL. CIV. CODE § 1798.81.5(b); Mass. Gen. Laws ch. 93H § 2(a); Conn. Gen. Stat. § 42-520(a)(3). Some, including Nevada, require encryption for certain sensitive information. *E.g.*, N.R.S. 603A.215 (encryption requirements for businesses that accept payment cards); Conn. Gen. Stat. § 42-470(b)(3) (2022) (requiring encryption for transmission of Social Security numbers). Violations can yield steep penalties, like the California Attorney General's $148 million fine to Uber for exposing 57 million people's data.[38]

Even former intelligence officials agree. Former NSA head Admiral Michael Rogers has stated: "If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things."[39] Other prominent former government officials, including a former NSA Director and the Director of National Intelligence, a former Homeland Security Secretary, and a former Deputy Defense Secretary, have likewise publicly embraced the increased use of encryption.[40] This

---

[38] Press Release, Cal. Att'y Gen., California Attorney General Becerra, *San Francisco District Attorney Gascón Announce $148 Million Settlement with Uber over 2016 Data Breach and Cover-Up* (Sept. 26, 2018), https://oag.ca.gov/news/press-releases/california-attorney-general-becerra-san-francisco-district-attorney-gasc%C3%B3n.

[39] Atlantic Council, *US Cybercom And The NSA: A Strategic Look with ADM Michael S. Rogers*, YouTube (Jan. 21, 2016), http://www.youtube.com/watch?v=wnTGO6OFgCo.

[40] Mike McConnell, Michael Chertoff & William Lynn, *Why the Fear Over Ubiquitous Data Encryption is Overblown*, Wash. Post (July 28, 2015),

stance is particularly striking given that their government work involved, in large part, *exploiting* the absence of encryption in worldwide communications.

F. The importance of encryption to protect privacy is recognized globally.

The United Nations High Commissioner for Human Rights recently affirmed the key role of encryption for privacy and security and human rights, outlining the various ways it helps protect people:

> Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination. Encryption ensures that people can share information freely, without fear that their information may become known to others, be they State authorities or cybercriminals.[41]

Just last month, the European Court of Human Rights rejected a Russian law that prevented messaging companies from offering end-to-end encryption to their users, much as the State seeks to do here for children of Nevada. "In so far as this legislation permits the public authorities to have access, on a generalized basis and without sufficient safeguards, to the content of electronic communications," the court concluded, "it impairs the very essence of the right to respect for private life

---

https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

[41] U.N. High Comm'r for Human Rights, 51st Sess., U.N. Doc. A/HRC/51/17, at 6 (Aug. 4, 2022), https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf?token=kicDzL656nY4jBZ4A1&fe=true.

under Article 8 of the [European] Convention [on Human Rights]." *Podchasov v. Russia*, No. 33696, 2024 HUDOC at *80 (Eur. Ct. H.R. 2024) https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}. This Court should similarly reject the State's attempt to impair the privacy rights of Nevadans here.[42]

II. Law enforcement can and does effectively conduct investigations into crimes involving end-to-end encrypted communications services.

Protecting children from abuse is rightfully a high priority, which is why this Court should reject the State's proposal to put children at serious risk from a wider range of threats. Moreover, introducing these risks is largely unnecessary, as Messenger's design gives law enforcement many other ways to obtain information about suspect communications between minors and adults.

At the outset, it is important to correct the State's mischaracterization of CyberTipline data. The CyberTipline's operator states that over 99.5 percent of the reports it received in 2022 involved suspected *imagery* of child abuse, not abusive contacts between adults and children.[43] Additionally, over half of the reports from

---

[42] The State's demand would also impact adults and residents of other states who are communicating with Nevada minors, since every participant in a conversation has to have E2EE turned on for the feature to work.

[43] Nat'l Ctr. for Missing & Exploited Children, *CyberTipline 2022 Report* (2022), https://urldefense.com/v3/__https:/www.missingkids.org/cybertiplinedata__;!!Phyt6w!ab-dTYoKYx9qyFm_tQoX0wK7Yl8aLT75yQm-CG_T-068pkC0D8Ih1wvlnHw1Lh692MOaPXvChf1vtAJy$https://www.missingkids.org/

tech companies were not actionable, for example because they involved imagery that is "viral and has been reported multiple times."[44] Thus, there is no data to support the inflammatory and irresponsible claim that two children are victimized on either Facebook or Instagram (which use Messenger for direct messaging) every day in Nevada.

Without the hyperbole and misrepresentations, it becomes clearer how unreasonable it is to ask that billions of messages be left unsecured so that police have an easier time, even as additional billions of messages on other popular services remain inaccessible to police.

Nevada law enforcement has many other ways to get information about suspect communications between minors and adults suspected of criminal behavior—including subpoenaing Meta for communications metadata through standard legal processes, obtaining the content from the victims themselves, or obtaining the content from anyone to whom the victim or perpetrator has forwarded it. Nevada also admits, as it must, that it has purchased forensic tools that can retrieve and analyze phone contents, albeit not in every single case. [45]

---

cybertiplinedata.

[44] *Id.*

[45] Logan Koepke et al., Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones 35, 38, 78 (2020), https://www.upturn.org/work/mass-extraction/ (Las Vegas Metropolitan Police Department has spent at least $646,000 on a variety of mobile device forensics tools).

Meta is a major information source for law enforcement. It gathers so much information about its users that it is capable of detecting unsafe activity without monitoring the contents of users' private communications. *Amici* consider this extensive information-gathering to be a continuing shortcoming for user privacy. But the practice does allow Meta to employ methods for detecting online abuse that do not rely on at-will access by providers to their users' communications content, such as metadata analysis, in which Meta engages, as well as enabling users to report abusive interactions.[46]

In a peer-reviewed study authored by *amica* Pfefferkorn, a survey of online service providers (including Meta) revealed that these "content-oblivious" techniques (especially user reporting)—which are not affected by E2EE—are considered more useful than monitoring the contents of users' communications when it comes to detecting nearly every kind of online abuse, including hate speech, harassment, and self-harm content, categories of particular concern in the State's Complaint. *E.g.*, Compl. ¶¶ 239-246, 369, 372. Importantly, for detecting attempts to sexually exploit children online, such as grooming and enticement—i.e., the motivation for the State's PI request—Pfefferkorn's study found that user reporting is considered just as useful as scanning communications contents.

[46] Riana Pfefferkorn, *Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers*, 1 J. Online Trust & Safety 1, 3, 17 (2022).

Further, only private messaging on Messenger, WhatsApp, and Instagram are E2EE. Information that people post on Facebook—including photos, posts, groups, and more—is not securely encrypted, and is accessible to law enforcement with proper legal process. What's more, the unencrypted metadata that Meta collects can show identity, who a user communicates with and how frequently, and more.[47] This enables the State to obtain voluminous user data from Meta, despite its representations to the contrary. Pl's Mot. for TRO and Prelim. Inj. Ex. 2 (Gonzales Decl. at ¶¶ 14, 21). Indeed, according to the company's transparency reports, Meta routinely hands over user data in response to U.S. law enforcement agencies' legal requests, to the tune of tens of thousands of requests every six months – and the numbers just keep going up.[48] Even now that Messenger chats are E2EE by default, "Meta will continue to provide message and call logs, as well as IP data."[49]

---

[47] Meta, *Government Requests for User Data: Further Asked Questions*, https://transparency.fb.com/reports/government-data-requests/further-asked-questions/ (stating that Meta may produce data including a user's name and email address, "login/logout IP addresses," message headers and IP addresses, and stored account contents "[s]uch as messages, photos, videos, timeline posts, and location information").

[48] Meta, *Government Requests for User Data: United States*, Meta Transparency Center, https://transparency.fb.com/reports/government-data-requests/country/US/https://transparency.fb.com/reports/government-data-requests/country/US/. The transparency reports do not break out legal requests by specific Meta product.

[49] Meta, *U.S. Legal Process Requirements*, https://about.meta.com/actions/safety/

In short, Meta no longer has access to its users' private conversations, yet it gathers so much information on its users that can still combat bad actors' attempts to prey on child users of Messenger. Nevada cannot say that end-to-end encryption always blocks investigations, but instead that end-to-end encryption may make its investigative efforts more difficult on occasion. On the other side, the State's proposed solution is to prevent Meta from offering the additional protections that end-to-end encryption provides for all of its minor users, lest those protections make law enforcement's occasional need for access to the content of their messages more difficult.

It would be naïve to claim that E2EE will never interfere with criminal prosecutions, even as encryption proponents demonstrate that the technology prevents a large amount of crime from happening in the first place. Police would also have an easier time if we dispensed with the warrant requirement, allowed questioning without attorneys present, or otherwise dispensed with due process, civil rights and other safeguards. But that is not the way our system of government works.

CONCLUSION

For the foregoing reasons, this Court should deny Nevada's motion for a

---

audiences/law/guidelines/.

preliminary injunction. Dated this 11th day of March, 2024.

/s/ Christopher M. Peterson
CHRISTOPHER M. PETERSON, ESQ. (13932)
AMERICAN CIVIL LIBERTIES
UNION OF NEVADA
4362 W. Cheyenne Ave.
North Las Vegas, NV 89032
Telephone: (702) 366-1226
Facsimile: (702) 830-9205
Emails: peterson@aclunv.org

Attorney for Amici Curiae

JENNIFER STISA GRANICK, ESQ.*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
425 California St., 7th Fl.
San Francisco, CA 94104
Telephone: 415-343-0758
Email: jgranick@aclu.org
**Pro hac vice* forthcoming

CERTIFICATE OF COMPLIANCE

1. I hereby certify that this brief complies with the formatting requirements of NRAP 32(a)(4), the typeface requirements of NRAP 32(a)(5) and the type style requirements of NRAP 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using **Microsoft Word Processing Program** in **size 14, Times New Roman font type**;

2. I further certify that this brief complies with the page- or type-volume limitations of NRAP 32(a)(7) because, excluding the parts of the brief exempted by NRAP 32(a)(7)(C), it is proportionately spaced, has a typeface of 14 points or more, and contains **6215** words;

3. Finally, I hereby certify that I have read this appellate brief, and to the best of my knowledge, information, and belief, it is not frivolous or interposed for any improper purpose. I further certify that this brief complies with all applicable Nevada Rules of Appellate Procedure, in particular NRAP 28(e)(1), which requires every assertion in the brief regarding matters in the record to be supported by a reference to the page and volume number, if any, of the transcript or appendix where the matter relied on is to be found. I understand that I may be subject to sanctions in the event that the accompanying brief is not in conformity with the requirements of the Nevada Rules of Appellate Procedure.

Dated this 11th day of March, 2024.

/s/ Christopher M. Peterson
CHRISTOPHER M. PETERSON, ESQ. (13932)
AMERICAN CIVIL LIBERTIES UNION OF NEVADA
4362 W. Cheyenne Ave.
North Las Vegas, NV 89032
Telephone: (702) 366-1226
Facsimile: (725) 210-6328
Emails: peterson@aclunv.org

Attorney for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that on the 11th day of March, 2024, I served a true and correct copy of the foregoing **Brief of *Amici Curiae* American Civil Liberties Union, American Civil Liberties Union of Nevada, et al. in Support of Defendant Meta Platforms** via the Court's electronic filing system only, pursuant to the Nevada Electronic Filing and Conversion Rules, Administrative Order 14-2, to all parties currently on the electronic service list.

/s/ Christopher M. Peterson
CHRISTOPHER M. PETERSON, ESQ. (13932)
AMERICAN CIVIL LIBERTIES
UNION OF NEVADA
4362 W. Cheyenne Ave.
North Las Vegas, NV 89032
Telephone: (702) 366-1226
Facsimile: (725) 210-6328
Emails: peterson@aclunv.org

Attorney for Amici Curiae

EXHIBIT A

Subject: Re: Amici Curiae Brief in Nevada v. Meta A-24-886110-B
Date: Tuesday, March 5, 2024 at 5:00:58 PM Pacific Standard Time
From: Mark J. Krueger
To: Jennifer Granick
CC: Brett Max Kaufman, Chris Peterson, Andrew Crocker

Ms. Granick,

Thank you again for your email. I have discussed your request internally and provide the following for your consideration. The State would conditionally consent to the filing of a joint amicus brief by the ACLU, the state ACLU, and the EFF if you all would agree to file the motion and amicus brief on or before Monday, March 11, 2024.

The reason for the specific date is that the State has concerns about the timing of your requested filing date. The issue that is being briefed before the district court is on a condensed briefing schedule, which is almost never the case in the Nevada Supreme Court. The rules that you cite are applicable to appellate court procedure with briefing schedules and hearing dates that are considerably longer than the briefing schedule we have in our district court case.

The State's reply brief is due the day of your proposed filing date. Therefore, our suggested date for the filing of your amicus brief of March 11, 2024, would allow the State at least some opportunity to review your amicus brief and incorporate any responses as necessary that the State may have into the State's reply brief.

Please let me know if you all are in agreement to this proposal including the filing date, and we can formalize the State's consent.

Thank you,
Mark
Cell 775-600-3504

Mark J. Krueger
Chief Deputy Attorney General
and Consumer Counsel
Bureau of Consumer Protection
Nevada Attorney General's Office
100 N. Carson Street

EXHIBIT B

Subject: RE: Statement of consent to file
Date: Monday, March 11, 2024 at 4:20:15 PM Pacific Daylight Time
From: Shafroth, Nathan
To: Jennifer Granick
Attachments: image001.png

Hi Jennifer. You have Meta's consent to file an amicus brief.

Nate

Nathan Shafroth

Covington & Burling LLP
Salesforce Tower, 415 Mission Street, Suite 5400
San Francisco, CA 94105-2533
T +1 415 591 7053 | nshafroth@cov.com
www.cov.com

COVINGTON

From: Jennifer Granick <jgranick@aclu.org>
Sent: Monday, March 11, 2024 4:17 PM
To: Shafroth, Nathan <nshafroth@cov.com>; Jackson, Gavin <GJackson@cov.com>; Joyner, Nia <NJoyner@cov.com>; Robyn Greene <robyngreene@meta.com>
Subject: Statement of consent to file

[EXTERNAL]
Hello,

For our filing today, we need a short statement that we have Meta's consent to file an amicus. Could someone provide this to me right away, please?

Thank you.