Wir unterstützen den Entwurf einer Verordnung zur Prävention und Bekämpfung sexueller Gewalt an Kindern online

Sehr geehrte Mitglieder des Europäischen Parlaments,

Sehr geehrte Vertreterinnen und Vertreter der Mitgliedstaaten im Rat der Europäischen Union,

die Unterzeichnenden unterstützen nachdrücklich den Vorschlag für eine Verordnung zur Prävention und zur Bekämpfung sexueller Gewalt von Kindern online, der derzeit von der EU beraten wird.

Wir erinnern alle Beteiligten daran, dass große Teile der Verordnung lediglich darauf abzielen, Praktiken zum Schutz von Kindern dauerhaft transparenter und rechenschaftspflichtig zu regeln. Einige Internetunternehmen praktizieren diese bereits seit 2009 auf freiwilliger Basis. Die Verordnung wird diese Kinderschutzpraktiken und die Nutzung aller damit verbundenen technischen Hilfsmittel in einen klar definierten, transparenten und rechenschaftspflichtigen Rechtsrahmen setzen.

Die erwähnten Praktiken zum Schutz von Kindern wurden von der EU in der am 14. Juli 2021 vereinbarten befristeten Ausnahmeregelung ausdrücklich gebilligt. Sie wird am 3. August 2024 auslaufen. Vor der Verabschiedung der befristeten Ausnahmeregelung setzten einige Unternehmen ihre bisherigen Tätigkeiten aus. Dies führte zu einem Rückgang der Gesamtzahl der in der EU eingegangenen Meldungen über sexuelle Gewalt an Kindern online um 58 %.

Wenn die Verordnung nicht bis zum 3. August 2024 verabschiedet wird, wissen wir mit großer Sicherheit, was passieren wird. Der Einsatz von Kinderschutzinstrumenten zur Aufdeckung von sexueller Gewalt an Kindern im Internet wird EU-weit in Kommunikationsdiensten verboten werden. Dabei handelt es sich um die Dienste, die von Straftäter*innen am häufigsten genutzt werden, um Material der sexuellen Gewalt an Kindern online auszutauschen und Kontakte zu Kindern in sexueller Absicht anzubahnen (grooming). Die auf diese Weise eingegangenen Meldungen machen mindestens 80 % aller in der EU eingegangenen Meldungen über sexuelle Gewalt an Kindern online aus. Im Jahr 2022 waren dies 1,5 Millionen Einzelmeldungen. Wenn diese Verordnung nicht verabschiedet wird, werden viele Kinder gefährdet werden. Das darf nicht passieren.

Diese Berichte sind unerlässlich, um gefährdete Kinder zu identifizieren und vor laufender oder drohender Gewalt zu schützen, um eine erneute Viktimisierung durch die fortgesetzte Verbreitung von Bildern oder Videos von sexueller Gewalt an Kindern zu verhindern und um den Strafverfolgungsbehörden zu helfen, die Täter*innen zu fassen. Wenn diese Berichte verloren gehen, wird dies schreckliche Folgen für Kinder haben die sexuelle Gewalt erfahren haben, nicht nur in jedem EU-Mitgliedstaat, sondern auch weit darüber hinaus.

- **Prävention ist ein wichtiger Schwerpunkt der Verordnung**
  Ein wesentlicher Teil der Verordnung ist die Forderung nach Risikobewertungen und Maßnahmen zur Risikominderung im Zusammenhang mit der Sicherheit von Kindern. Dadurch soll verhindert werden, dass Kinder durch sexuelle Gewalt geschädigt, die Aufdeckung von Online-Grooming-Verhalten erleichtert und das Risiko der Viktimisierung verringert werden.

  Verpflichtende Aufdeckungsanordnungen sind ein letztes Mittel, welches nur zum Einsatz kommt, wenn die zur Verhinderung von sexueller Gewalt ergriffenen Risikominderungsmaßnahmen als unzureichend erachtet werden.

- **Die Aufdeckung durch die Unternehmen ist für den Schutz der Kinder unerlässlich**
  Darstellungen sexueller Gewalt an Kindern (CSAM) ist ein Beweis für ein Verbrechen gegen Kinder, und in der Online-Welt sind Unternehmen wichtige Partner für deren Aufdeckung und Meldung an die Strafverfolgungsbehörden.

  Es ist allgemein bekannt, dass Kinder ihre Gewalterfahrung oft nie oder erst im Erwachsenenalter offenlegen. Zu diesem Zeitpunkt kann sich der in der Kindheit erlittene Schaden vergrößert und komplexe Formen angenommen haben. Kinder sind sich oft nicht bewusst, dass sie sexuelle Gewalt erfahren, oder sind sich der Schäden nicht bewusst, die mit der Veröffentlichung von sexualisierten Bildern von ihnen im Internet verbunden sind. Auch Eltern und Betreuer*innen erkennen möglicherweise die Anzeichen und Symptome von sexueller Gewalt an Kindern nicht, oder sie sind selbst die Täter*innen. Die Ausweitung der Möglichkeiten zur Meldung von sexueller Gewalt für Kinder und die Aufklärung der Eltern und der Öffentlichkeit über Online-Sicherheit sind notwendig, aber nicht ausreichend, um sexuelle Gewalt an Kindern im Internet in großem Umfang zu verhindern.

- **Verpflichtungen zur Prävention und Bekämpfung der sexuellen Gewalt an Kindern sind von entscheidender Bedeutung**
  Da Vorbeugung, Aufdeckung und Meldung derzeit auf freiwilliger Basis erfolgen, gibt es wenig oder keine rechtlich fundierte Transparenz. Zu viele Unternehmen haben sich dafür entschieden, überhaupt nichts für den Schutz von Kindern zu tun, oder es gibt erhebliche Unstimmigkeiten in ihrem Vorgehen.

  Die Verordnung wird den Schutz von Kindern im Internet erheblich verbessern, da alle einschlägigen Online-Unternehmen einer sorgfältig definierten, öffentlich nachvollziehbaren rechtlichen Regelung unterliegen werden.

- **Die verpflichtende Aufdeckungsanordnung wird zu technologischen Verbesserungen in den Unternehmen führen**
  Jede Software, jedes Programm, kann stufenweise verbessert werden. Aber die Verbesserungen entstehen durch sorgfältige Überwachung, Rückkopplungsschleifen und durch verbindliche Transparenzmechanismen, welche die Verordnung einführen wird. Verbesserungen kommen nie zustande, wenn die Programme oder Werkzeuge nie eingesetzt werden.

- **Einige der verfügbaren, effektiven Tools werden seit über einem Jahrzehnt eingesetzt**
  PhotoDNA war das erste Perceptual-Hashing-Tool, das in großem Umfang zur Identifizierung von Materialien sexueller Gewalt an Kindern online eingesetzt wurde. Es steht seit 2009 zur Verfügung und hat sich bei der Identifizierung von mehreren Millionen Bildern von sexueller Gewalt an Kindern in der ganzen Welt als äußerst erfolgreich erwiesen.

  Keine der apokalyptischen Visionen, die während der Debatte über die befristete Ausnahmeregelung oder in der Debatte über die Verordnung gezeichnet wurden, sind eingetreten. Das werden sie auch nicht.

- **Strafverfolgungsbehörden begrüßen Meldungen von Unternehmen**
  Die Polizei wird nicht mit Falschmeldungen überschwemmt. Im Gegenteil, die Strafverfolgungsbehörden schätzen die Art und Weise, in der PhotoDNA und andere Tools ihnen bei der wichtigen Aufgabe helfen, Kinder zu schützen.

- **Schnelles Handeln ist entscheidend**
  Die Polizeibehörden können nicht immer sofort auf die bei ihnen eingehenden Meldungen reagieren. In einem Betroffenenorientierten, ganzheitlichen Rahmen ist jedoch die schnellstmögliche Identifizierung und Entfernung von CSAM aus dem Internet von entscheidender Bedeutung, und dasselbe gilt für schnelles Handeln, um ein Kind auf die Gefahren des Grooming aufmerksam zu machen. Dadurch kann verhindert werden, dass dem Kind unermesslicher Schaden zugefügt wird.

  Die Entfernung von illegalem Material und die Verhinderung von Grooming ergänzen und unterstützen polizeiliche Maßnahmen.

- **Die Genauigkeitsrate ist außergewöhnlich hoch und wird sich weiter verbessern**
  PhotoDNA arbeitet mit einer Genauigkeitsquote von schätzungsweise nur einem falsch positiven Ergebnis bei 50 Milliarden gescannten Bildern. Bei der Erkennung von neuem, bisher ungesehenem Material sexueller Gewalt an Kindern erreichen die Fähigkeiten neuer Formen der KI bereits eine Schwelle von 99,9 %. Angesichts der KI-Revolution, die wir gerade erleben, werden sie sich wahrscheinlich noch weiter verbessern. In den neuen Regelungen, die in der Verordnung vorgesehen sind, wird das neue Europäische Zentrum speziell dafür zuständig sein, sicherzustellen, dass falsch-positive Ergebnisse eliminiert und nicht an die Strafverfolgungsbehörden weitergegeben werden.

  Dies ist eine weitaus bessere Regelung als der Status quo, bei dem die wenigen Unternehmen, die sich für die Einführung automatischer Erkennungsmaßnahmen entscheiden, nicht verpflichtet sind, die Genauigkeit ihrer Berichte zu gewährleisten oder zu verbessern.

- **Die Ende-zu-Ende-Verschlüsselung ist in keiner Weise gefährdet.**
  Keines der derzeit verwendeten oder geplanten Instrumente zum Schutz von Kindern ist in der Lage, etwas anderes als CSAM oder Aktivitäten, die mit hoher Wahrscheinlichkeit mit sexueller Gewalt an Kindernin Verbindung stehen, zu sehen, zu lesen, zu verstehen oder zu identifizieren.

  Die Technologien können lediglich Muster der Gewalt an Kindern erkennen, bevor entsprechende Darstellungen oder Kommunikationen in den verschlüsselten Tunnel gelangen, woraufhin sie verloren sind. Solche oder ähnliche Werkzeuge werden seit vielen Jahren in Verbindung mit Ende-zu-Ende-verschlüsselten Diensten eingesetzt, um beispielsweise Nutzer*innen zu warnen, dass ein potenzieller Link von einem Betrüger stammen könnte.

- **Wir dürfen die Rechtsstaatlichkeit nicht untergraben**
  Ein Verbot der Verwendung von Kinderschutz-Mechanismen in Verbindung mit Apps, die eine Ende-zu-Ende-Verschlüsselung verwenden, wäre gleichbedeutend mit der Ankündigung, dass die EU die Schaffung eines riesigen virtuellen Raums zulässt, der sich dem Zugriff von Gesetzen, Strafverfolgungsbehörden und Gerichten entzieht.

  Aufgrund des Ausmaßes der Herausforderung bedroht das Verbot der Verwendung von Kinderschutz-Mechanismen in Verbindung mit Ende-zu-Ende-verschlüsselten Umgebungen die Idee der Rechtsstaatlichkeit. Straftäter*innen werden ihre Aktivitäten über verschlüsselte

Anwendungen verstärken, weil sie glauben, dass sie ungestraft handeln können. Und in der überwiegenden Mehrheit der Fälle werden sie Recht haben. Sie können es.

- **Es geht nicht nur um das Dark Web**
  Straftäter*innen gehen dorthin, wo Kinder sind. Kinder sind nicht im Dark Web unterwegs. Aus diesem Grund sind nicht alle Täter*innen als Reaktion auf die erweiterten Kinderschutzmaßnahmen im Internet ins Dark Web abgewandert. Es ist zweifellos richtig, dass große Mengen von CSAM über Dark-Web-Dienste ausgetauscht werden, aber ein großer Teil dieser Bilder stammt aus dem Internet oder ist dort gelandet. Es geht nicht darum, ob man das Internet oder das Dark Web bekämpfen soll. Beide müssen angegangen werden.

- **Die öffentliche Meinung unterstützt die Verordnung sehr stark**
  Wir alle akzeptieren, dass unsere persönlichen Gegenstände, sogar unsere Körper, auf Flughäfen oder am Eingang zu sensiblen Gebäuden massenhaft gescannt oder kontrolliert werden. Wir tun dies, weil wir den zugrundeliegenden sozialen Zweck des allgemeinen Schutzes verstehen und akzeptieren.

  Ebenso besteht kein Zweifel daran, dass die breite öffentliche Meinung in den EU-Mitgliedstaaten die im Verordnungsentwurf vorgesehenen Maßnahmen befürwortet.

Unterzeichnet haben wie folgt. (Die vollständige Liste der Unterzeichner*innen wird zu gegebener Zeit im Internet veröffentlicht). Unter den Erstunterzeichnenden sind:

Ajda Petek	Faculty of Social Sciences, University of Ljubljana, Safer Internet Centre Slovenia
Andrea Cox	digiQ (civil society organisation), Director
Andrew Campling	Director, 419 Consulting Ltd and Trustee, Internet Watch Foundation
Asha Anderson	Ostia
Ashley Woodfall	Bournemouth University, Senior Principal Academic
Astrid Winkler	ECPAT Austria, Executive Director
Bjørn-Erik Ludvigsen	Norwegian NC3, Police Superintendent
Catherine Blaya	Université Côte d'Az Founder and Chief Technical Officer ur, Pr
Bruce Ramsay	Cyacomb,
Camille Cooper	Augusta Associates LLC, CEO
Dr. Cary Bazalgette	University College London Institute of Education
Prof. Charo Sádaba	University of Navarra, School of Communication
Prof. doc. Mag. Dr.Christine Trültzsch-Wijnen	Salzburg University of Education, Stefan Zweig & Charles University
Costas Yannopoulos	The Smile of the Child, President, Board of Directors
Prof. Cristina Ponte	Universidade Nova de Lisboa
Prof. Daryl J Higgins	Institute of Child Protection Studies, Australian Catholic University

Dave Ranner	CameraForensics, Director
Dawn Hawkins	National Center on Sexual Exploitation, CEO
Deepa Limbu Subba	ECPAT Luxembourg, Executive Director
Dr. Rebecca Portnoff	Thorn, Head of Data Science
Edward Dixon	Rigr AI
Dr. Elien De Caluwé	Tilburg University
Elizabeth Gosme	COFACE Families Europe, Director
Prof. Elizabeth J. Letourneau	Moore Center for the Prevention of Child Sexual Abuse, Director
Prof. Ellen Helsper	LSE, Professor of Digital Inequalities
Prof. Ernesto Caffo	University of Modena and Reggio Emilia
Prof. Ethel Quayle	University of Edinburgh
Fabiola Bas Palomares	Eurochild, Policy & Advocacy Officer - Online Safety
Dr. Félix Ortega	Universidad de Salamanca / University of Salamanca
Francisca De Magalhães Barros	Universidade Autónoma de Lisboa, Activista dos Direitos Humanos
Gary Ellis, PhD	The University of Guelph-Humber, Head of School-Justice Studies
Associate Professor Gianna Cappello	University of Palermo
Associate Professor Giovanna Mascheroni	Università Cattolica del Sacro Cuore
Gretchen Peters	Alliance to Counter Crime Online, Executive Director
Guillaume Landry	ECPAT International, Executive Director
Prof. Hany Farid	University of California, Berkeley
Heidi Als Ringheim	Int. Academy of Sexology & RelationshipTherapy, Sexologist and Relationship Therapist
Ian Stevenson	OSTIA (Online Safety Technology Industry Association), Chair
Prof. Ilan Talmud	University of Haifa
Jarmila Kubáňková, Ph.D.	Cesta z krize, z. ú.
Jessica Airey	Brave Movement, Europe Campaign Manager
John Carr	Children's Charities' Coalition on Internet Safety
Jorge Flores Fernández	PantallasAmigas, Founder
Dr. Juan Arraiza	European Anti-Cybercrime Technology Development Association
Julia von Weiler	Innocence in Danger e.V., Psychologist / CEO
Julie Cordua	Thorn
Jutta Croll, M.A.	Stiftung Digitale Chancen / Digital Opportunities Foundation, Germany
Kateřina Klapilová, Ph.D. (ECPS)	Chaerles University and National Institute of Mental Health
Lavinia Liardo	Terre des Hommes International Federation, Head EU Policy and Advocacy
Lianna McDonald	Canadian Centre for Child Protection, Executive Director
Lori Cohen	Protect All Children from Trafficking, Chief Executive Officer

Prof. M Catherine Maternowska	University of Edinburgh, Professor of Violence Prevention
Marija Manojlovic	Safe Online Fund / End Violence Partnership, Director
Mark Pope	CameraForesics
Matt Burns	CEO, CameraForensics
Minne De Boeck	University of Antwerp / University Forensic Centre, Criminologist
Nathan Trevivian	Private Industry Expert: CameraForensics
Prof. Nicholas Blagden	University of Derby
Paul King	INTERPOL Specialists Group on Crimes Against Children, Researcher
Peter Wanless	NSPCC, CEO
Dr. Petros Daras	CERTH/ITI
Ray Genoe	University College Dublin, Director of the UCD Centre for Cybersecurity and Cybercrime Investigation
Richard Collard	NSPCC, Head of Child Safety Online
Seán Gaines	Fundación Centro de Tecnologías de Interacción Visual y Comunicaciones, Director of International Projects
Sharon Pursey OBE	SafeToNet Ltd
Simon Bailey CBE	Anglia Ruskin University, Chair of Policing Institute for the Eastern Region
Prof. Sonia Livingstone	London School of Economics and Political Science, Professor of Social Psychology
Sónia Rodrigues	NGO AjudAjudar and University Lusíada of Porto, President of the Board and researcher
Stefanos Vrochidis	ITI-CERTH, Senior Researcher
Steven Ormston	Polish Platform for Homeland Security, Communication & Community Manager
Susie Hargreaves OBE	Internet Watch Foundation (IWF), CEO
Tito de Morais	MiudosSegurosNa.Net, Founder
Torsten Krause	Digital Opportunities Foundation Germany, Political Scientist and Child Rights Researcher
Dr. Ute Navidi	independent international consultant
Prof. Veronika Kalmus	University of Tartu
William Wiltse	Child Rescue Coalition, President
Yiannis Laouris	CyberEthics Safer Internet Center, Future Worlds Center, Lead Scientist
John Shehan	National Center for Missing & Exploited Children (NCMEC), Senior Vice President
Carme Tello Casany	Federación de Asociaciones para la Prevención del Maltrato Infantil fapmi-ECPAT Spain, President
Prof. Julia Davidson OBE	University of East London
Narine Khachatryan	Safe . am ., Executive Director
Ryan De Souza	ChildFund Alliance, Senior Advisor, Advocacy and Policy
Assist. Professor Konstantinos Demestichas	Agricultural University of Athens
Ask Hesby Krogh	Digitalt Ansvar - Digital Accountability, director

Mie Oehlenschlager	Tech & Childhood, founder
Lydia Konstantinova Zagorova	Member of ECPAT.International and Member of the Board of SCARS,.USA, Director of ECPAT Bulgaria - Neglected Children and Women Foundation
Mirjam Blaak	Defence for Children – ECPAT Netherlands, Executive Director
Victoria Green	CEO, Marie Collins Foundation
Kelly Schut	Free a Girl the Netherlands, Director
Samantha Morton	N/A, Actress
Teresa K. Jauregui	National Child Protection Task Force, Chief Legal Officer
Anna Karin Hildingson Boqvist	ECPAT Sweden, Secretary-General
Christopher Knibb	The Institution of Engineering and Technology
Fiona Jennings	The Irish Society for the Prevention of Cruelty to Children (ISPCC), Head of Policy and Public Affairs
Jasmin Abo Loha	It is possible but we need more time, General Secretary
Deborah Denis	The Lucy Faithfull Foundation, CEO
Şahin Antakyalıoğlu	ECPAT Türkiye, President
Cristiane Augusta da Silva Miranda	Agarrados à Net - Cofounder
Rebecca Portnoff	Head of Data Science, Thorn
Susie Hargreaves OBE	CEO, Internet Watch Foundation (IWF)