The text below is an open letter on the position of scientists and researchers on the recently proposed changes to the EU's proposed Child Sexual Abuse Regulation.

As of the 7th May 2024, the letter has been signed by 312 scientists and researchers from 35 countries.

For information on signing the letter, please see the end of this document.

For press inquiries please contact:

Carmela Troncoso - carmela.troncoso@epfl.ch (Spain, Switzerland)
Bart Preneel - bart.preneel@esat.kuleuven.be (Belgium)
Michael Veale - m.veale@ucl.ac.uk (UK)
René Mayrhofer - rm@ins.jku.at (Austria)
Aurélien Francillon - aurelien.francillon@eurecom.fr (France)
Eyal Ronen - eyal.ronen@cs.tau.ac.il (Israel)
TJ McIntyre - tjmcintyre@ucd.ie (Ireland)
Jaap-Henk Hoepman - jhh@cs.ru.nl (The Netherlands)
Peter Schwabe - peter@cryptojedi.org (Germany)
Diego F. Aranha - dfaranha@cs.au.dk (Denmark)

Dear Members of the European Parliament,
Dear Member States of the Council of the European Union,

Joint statement of scientists and researchers on EU's new proposal for the Child Sexual Abuse Regulation: 2nd May 2024

We are writing in response to the new proposal for the regulation introduced by the Presidency on 13 March 2024[1]. The two main changes with respect to the previous proposal aim to generate more targeted detection orders, and to protect cybersecurity and encrypted data. We note with disappointment that these changes fail to address the main concerns raised in our open letter from July 2023 regarding the unavoidable flaws of detection techniques and the significant weakening of the protection that is inherent to adding detection capabilities to end-to-end encrypted communications. The proposal's impact on end-to-end encryption is in direct contradiction to the intent of the European Court of Human Rights's decision in *Podchasov v. Russia* on 13 February, 2024. We elaborate on these aspects below.

Child sexual abuse and exploitation are serious crimes that can cause lifelong harm to survivors; certainly it is essential that governments, service providers, and society at large take major responsibility in tackling these crimes. The fact that the new proposal encourages service providers to employ a swift and robust process for notifying potential victims is a useful step forward.

However, from a technical standpoint, to be effective, this new proposal will also completely undermine communications and systems security. The proposal notably still fails to take into account decades of effort by researchers, industry, and policy makers to protect communications. Instead of starting a dialogue with academic experts and making data available on detection technologies and their alleged effectiveness, the proposal creates unprecedented capabilities for surveillance and control of Internet users. This undermines a secure digital future for our society and can have enormous consequences for democratic processes in Europe and beyond.

[1] Minor modifications have been leaked since, with no significant change and without changing the conclusions in this letter

1. The proposed targeted detection measures will not reduce risks of massive surveillance

The problem is that flawed detection technology cannot be relied upon to determine cases of interest. We previously detailed security issues associated with the technologies that can be used to implement detection of known and new CSA material and of grooming, because they are easy to circumvent by those who want to bypass detection, and they are prone to errors in classification. The latter point is highly relevant for the new proposal, which aims to reduce impact by only reporting "users of interest" defined as those who are flagged repeatedly (as of the last draft: twice for known CSA material and three times for new CSA material and grooming). Yet, this measure is unlikely to address the problems we raised.

First, there is the poor performance of automated detection technologies for new CSA material and for the detection of grooming. The number of false positives due to detection errors is highly unlikely to be significantly reduced unless the number of repetitions is so large that the detection stops being effective. Given the large amount of messages sent in these platforms (in the order of billions), one can expect a very large amount of false alarms (in the order of millions).[2]

Second, the belief that the number of false positives will be reduced significantly by requiring a small number of repetitions relies on the fallacy that for innocent users two positive detection events are independent and that the corresponding error probabilities can be multiplied. In practice, communications exist in a specific context (e.g., photos to doctors, legitimate sharing across family and friends). In such cases, it is likely that parents will send more than one photo to doctors, and families will share more than one photo of their vacations at the beach or pool, thus increasing the number of false positives for this person. **It is therefore unclear that this measure makes any effective difference with respect to the previous proposal**.

Furthermore, to realize this new measure, on-device detection with so-called client-side scanning will be needed. As we previously wrote, once such a capability is in place, there is little possibility of controlling what is being detected and which threshold is used on the device for such detections to be considered "of interest". We elaborate below.

High-risk applications may still indiscriminately affect a massive number of people. A second change in the proposal is to only require detection on (parts of) services that are deemed to be high-risk in terms of carrying CSA material. This change is unlikely to have a useful impact. As the exchange of CSA material or grooming only requires standard features that are widely supported by many service providers (such as exchanging chat messages

[2] Given that there has not been any public information on the performance of the detectors that could be used in practice, let us imagine we would have a detector for CSAM and grooming, as stated in the proposal, with just a 0.1% False Positive rate (i.e., one in a thousand times, it incorrectly classifies non-CSAM as CSAM), which is much lower than any currently known detector. Given that WhatsApp users send 140 billion messages per day, even if only 1 in hundred would be a message tested by such detectors, there would be **1.4 million false positives every single day**. To get the false positives down to the hundreds, statistically one would have to identify at least 5 repetitions using different, statistically independent images or detectors. And this is only for Whatsapp - if we consider other messaging platforms, including email, the number of necessary repetitions would grow significantly to the point of not effectively reducing the CSAM sharing capabilities.

and images), this will undoubtedly impact many services. Moreover, an increasing number of services deploy end-to-end encryption, greatly enhancing user privacy and security, which will increase the likelihood that these services will be categorised as high risk. This number may further increase with the interoperability requirements introduced by the Digital Markets Act that will result in messages flowing between low-risk and high-risk services. As a result, almost all services could be classified as high risk.

This change is also unlikely to impact abusers. As soon as abusers become aware that a service provider has activated client side scanning, they will switch to another provider that will in turn become high risk; very quickly all services will be high risk, which defeats the purpose of identifying high risk services in the first place. And because open-source chat systems are currently easy to deploy, groups of offenders can easily set up their own service without any CSAM detection capabilities.

We note that decreasing the number of services is not even the crucial issue, as this change would not necessarily reduce the number of (innocent) users that would be subject to detection capabilities. This is because many of the main applications targeted by this regulation, such as email, messaging, and file sharing are used by hundreds of millions of users (or even billions in the case of WhatsApp).

Once a detection capability is deployed by the service, it is not technologically possible to limit its application to a subset of the users. Either it exists in all the deployed copies of the application, or it does not. Otherwise, potential abusers could easily find out if they have a version different from the majority population and therefore if they have been targeted. Therefore, upon implementation, the envisioned limitations associated with risk categorization **do not necessarily result in better user discrimination or targeting, but in essence have the same effect for users as a blanket detection regulation**.

2. Detection in end-to-end encrypted services by definition undermines encryption protection

The new proposal has as one of its goals to “protect cyber security and encrypted data, while keeping services using end-to-end encryption within the scope of detection orders”. As we have explained before, this is an oxymoron. The protection given by end-to-end encryption implies that no one other than the intended recipient of a communication should be able to learn any information about the content of such communication. Enabling detection capabilities, whether for encrypted data or for data before it is encrypted, **violates the very definition of confidentiality** provided by end-to-end encryption. Moreover, the proposal also states that “This Regulation shall not create any obligation that would require [a service provider] to decrypt or create access to end-to-end-encrypted data, or that would prevent the provision of end-to-end encrypted services.” This can be misleading, as whether the obligation to decrypt exists or not, the proposal undermines the protection provided by end-to-end encryption.

This has catastrophic consequences. It sets a precedent for filtering the Internet, and prevents people from using some of the few tools available to protect their right to a private life in the digital space; it will have a chilling effect, in particular to teenagers who heavily rely on online services for their interactions.[3,4] It will change how digital services are used around the world and is likely to negatively affect democracies across the globe. These consequences come from the very existence of detection capabilities, and thus cannot be addressed by either reducing the scope of detection in terms of applications or target users: once they exist, all users are in danger. Hence, the requirement of Art. 10 (aa) that "a detection order should not introduce cybersecurity risks for which it is not possible to take any effective measures to mitigate such risk" is not realistic, as the risk introduced by client side scanning cannot be mitigated effectively.

3. Introducing more immature technologies may increase the risk

The proposal states that age verification and age assessment measures will be taken, creating a need to prove age in services that before did not require so. It then bases some of the arguments related to the protection of children on the assumption that such measures will be effective. We would like to point out that at this time there is no established, well-proven technological solution that can reliably perform these assessments. The proposal also states that such verification and assessment should preserve privacy. We note that this is a very hard problem. While there is research towards technologies that could assist in implementing privacy-preserving age verification, none of them are currently in the market.[5] Integrating them into systems in a secure way is far from trivial. Any solutions to this problem need to be very carefully scrutinized to ensure that the new assessments do not result in privacy harms or discrimination causing more harm than the one they were meant to prevent.

4. Lack of transparency

It is quite regretful that the proposers failed to reach out to security and privacy experts to understand what is feasible before putting forth a new proposal that cannot work technologically. The proposal pays insufficient attention to the technical risks and imposes - while claiming to be technologically neutral - requirements that cannot be met by any state-of-the-art system (e.g., low false-positive rate, secrecy of the parameters and algorithms when deployed in a large number of devices, existence of representative simulated CSA material).

We strongly recommend that not only should this proposal not move forward, but that before such a proposal is presented in future, the proposers engage in serious conversations about what can and cannot be done within the context of guaranteeing secure communications for society.

5. Secure paths forward for child protection

Protecting children from online abuse while preserving their right to secure communications is critical. It is important to remember that CSAM *content* is the output of child sexual abuse. Eradicating CSAM relies on eradicating abuse, not only abuse *material.*[6] Proven approaches

[3] Teens and Internet, Device Access Fact Sheet
[4] Expert impact assessment on the initial version of the proposal
[5] European Parliament on Online age verification methods on children
[6] https://mit-serc.pubpub.org/pub/701yvdbh/release/2

recommended by organisations such as the UN[7] for eradicating abuse include education on consent,[8] on norms and values,[9] on digital literacy and online safety, and comprehensive sex education;[10] trauma-sensitive reporting hotlines; and keyword-search based interventions.[11] Educational efforts can take place in partnership with platforms, which can prioritise high quality educational results in search[12] or collaborate with their content creators to develop engaging resources.

We recommend substantial increases in investment and effort to support existing proven approaches to eradicate abuse, and with it, abusive material. Such approaches stand in contrast to the current techno-solutionist proposal, which is focused on vacuuming up abusive material from the internet at the cost of communication security, with little potential for impact on abuse perpetrated against children.

Signatories list below

[7] See https://www.unicef.org/eap/media/3686/file/Digital.pdf and https://www.unicef.org/eap/media/4706/file/What%20works.pdf

[8] https://www.gse.harvard.edu/news/uk/18/12/consent-every-age, https://theconversation.com/the-law-must-focus-on-consent-when-it-tackles-revenge-porn-29501

[9] https://www.togetherforgirls.org/wp-content/uploads/2019-11-15-What-Works-to-Prevent-Sexual-Violence-Against-Children-Evidence-Review.pdf

[10] See eg. , https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf, Graling, K. (2013). The Use and Misuse of Pleasure in Sex Education Curricula. Sex Education 13, no 5 (2013): 305-18.

[11] https://www.end-violence.org/sites/default/files/paragraphs/download/Global%20Threat%20Assessment%202019.pdf

[12] https://www.thestar.com.my/news/nation/2018/04/30/chatbot-to-help-with-sex-education-programme-can-answer-queries-as-well-as-connect-children-to-suppo

312 Signatories from 35 countries

Australia

Dr. Shaanan Cohney	University of Melbourne

Austria

Prof. Dr. Elena Andreeva	TU Wien
Prof. Roderick Bloem	Graz University of Technology
Prof. Maria Eichlseder	Graz University of Technology
Dr. Rainhard Dieter Findling	University of Applied Sciences Upper Austria
Prof. Daniel Gruss	Graz University of Technology
Prof. Clemens Heuberger	University of Klagenfurt
Prof. DI Dr. Martin Hitz	Alpen-Adria-Universität Klagenfurt
DI. Peter Kieseberg	St. Pölten University of Applied Sciences
Dr. Lukas Daniel Klausner	St. Pölten University of Applied Sciences
Prof. Martina Lindorfer	TU Wien
Prof. Dr. Robert Luh	St. Pölten University of Applied Sciences
Prof. Dr. Matteo Maffei	TU Wien
Prof. Stefan Mangard	Graz University of Technology
Prof. Dr. René Mayrhofer	Johannes Kepler University Linz
Prof. Dr. Klaus Miesenberger	Johannes Kepler University Linz
Prof. Dr. Silvia Miksch	TU Wien
Univ. Prof. Dr. Christian Rechberger	Graz University of Technology
Dr. Michael Roland	Johannes Kepler University Linz
Prof. Dr. Johannes Sametinger	Johannes Kepler University Linz
Prof. Peter Schartner	University of Klagenfurt

DI. Manfred Schlägl	Linz Institute of Technology
Prof. Edgar Weippl	University of Vienna
Prof. Angelika Wiegele	University of Klagenfurt

Belgium

Dr. Emad Heydari Beni	KU Leuven and Bell Labs
Dr. Rosamunde Van Brakel	Vrije Universiteit Brussel
Dr. Gaëtan Cassiers	UCLouvain
Dr. Lesly-Ann Daniel	KU Leuven
Prof. Claudia Diaz	KU Leuven
Prof. Dr. Gloria González Fuster	Vrije Universiteit Brussel
Dr. Benedikt Gierlichs	KU Leuven
Dr. Diane Leblanc-Albarel	KU Leuven
Dr. Thorben Moos	UCLouvain
Prof. Yves Moreau	KU Leuven
Prof. Jan Tobias Muehlberg	Université Libre de Bruxelles
Prof. Olivier Pereira	UCLouvain
Prof. Thomas Peters	UCLouvain & FNRS
Prof. Bart Preneel	KU Leuven
Prof. Jean-Jacques Quisquater	UCLouvain
Dr. Vera Rimmer	KU Leuven
Prof. Florentin Rochet	UNamur
Prof. Nigel Smart	KU Leuven and Zama
Prof. François-Xavier Standaert	UCLouvain
Prof. Mathy Vanhoef	KU Leuven
Prof. Ingrid Verbauwhede	KU Leuven

Brazil

Prof. Ian Brown	Personal capacity

Bulgaria

Ass. Prof. Vesselin Bontchev	Bulgarian Academy of Sciences

Canada

Dr. David Barrera	Carleton University
Prof. Ian Goldberg	University of Waterloo
Prof. Bailey Kacsmar	University of Alberta
Prof. Dr.-Ing. Florian Kerschbaum	University of Waterloo
Prof. Mohammad Mannan	Concordia University
Prof. Simon Oya	The University of British Columbia
Prof. Nicolas Papernot	University of Toronto and Vector Institute
Prof. Dr. Sebastian Schinzel	Privacy & Access Council of Canada

Czechia

Prof. Vashek Matyas	Masaryk University
Prof. Petr Svenda	Masaryk University

Denmark

Prof. Diego F. Aranha	Aarhus University
Prof. Carsten Baum	Technical University of Denmark
Prof. Ivan Damgård	Aarhus University
Prof. Rosario Giustolisi	IT University of Copenhagen
Prof. Christian Majenz	Technical University of Denmark

Prof. Jesper Buus Nielsen	Aarhus University
Prof. Claudio Orlandi	Aarhus University
Prof. Luisa Siniscalchi	Technical University of Denmark
Prof. Tyge Tiessen	Technical University of Denmark

Estonia

Dr. Levent Aksoy	Tallinn University of Technology
Dr. Dan Bogdanov	Estonian Academy of Sciences
Prof. Helger Lipmaa	University of Tartu

Finland

Prof. Kimmo Halunen	University of Oulu

France

Prof. Rémi Cogranne	Troyed University of Technology

Dr. Daniele Antonioli	EURECOM
Prof. Gildas Avoine	INSA Rennes
Prof. David Baelde	ENS Rennes, IRISA
Dr. Gustavo Banegas	Independent Researcher
Dr. Sébastien Bardin	CEA List, Université Paris-Saclay
Dr. Gregory Blanc	Institut Polytechnique de Paris
Dr. Bruno Blanchet	Inria
Dr. Xavier Bonnetain	Inria
Prof. Christina Boura	University of Versailles
Dr. Daniel De Almeida Braga	Inria
Dr. Sophie Chabridon	Institut Polytechnique de Paris
Dr. Brice Colombier	Université Jean Monnet, Saint-Étienne

Dr. Véronique Cortier	CNRS
Dr. Damien Couroussé	CEA List
Dr. Alexandre Debant	Inria
Dr. Stéphanie Delaune	CNRS
Dr. Jannik Dreier	Université de Lorraine
Dr. Barbara Fila	INSA Rennes
Prof. Aurélien Francillon	EURECOM
Dr. Aymeric Fromherz	Inria
Prof. Joaquin Garcia-Alfaro	Institut Polytechnique de Paris
Dr. Pierrick Gaudry	CNRS
Prof. Louis Goubin	Université de Versailles Saint-Quentin-en-Yvelines
Dr. Vincent Hugot	INSA Centre Val de Loire
Dr. Charlie Jacomme	Inria
Dr. Adrien Koutsos	Inria
Dr. Steve Kremer	Inria
Prof. Pascal Lafourcade	Université Clermont Auvergne
Dr. Joseph Lallemand	CNRS
Dr. Pierre Laperdrix	CNRS
Dr. Vincent Laporte	Inria
Dr. Gaëtan Leurent	Inria
Dr. Damien Marion	Rennes University
Dr. Stephan Merz	Inria
Dr. Camille Monière	Université Bretagne Sud
Dr. María Naya-Plasencia	Inria
Prof. Benjamin Nguyen	INSA Centre Val de Loire
Dr. Cristina Onete	University of Limoges
Dr. Léo Perrin	Inria

Dr. Yann Rotella	Université de Versailles Saint-Quentin-en-Yvelines, Paris-Saclay University
Dr. Merve Sahin	EURECOM
Dr. André Schrottenloher	Inria
Dr. Emmanuel Thomé	Inria
Dr. Jean-Pierre Tillich	Inria
Dr. Reda Yaich	Institut de Recherche Technologique SystemX
Prof. Melek Önen	EURECOM

Germany

Dr. Ali Abbasi	CISPA Helmholtz Center for Information Security
Prof. Dr. Florian Adamsky	Hof University of Applied Sciences
Prof. Dr. Sebastian Berndt	Technische Hochschule Lübeck
Dr.-Ing. Sven Bugiel	CISPA Helmholtz Center for Information Security
Dr.-Ing. Jiska Classen	Hasso-Plattner-Institute, University of Potsdam
Prof. Dr. Cas Cremers	CISPA Helmholtz Center for Information Security
Dr.-Ing. Daniel Demmler	Zama
Prof. Dr.-Ing. Alexandra Dmitrienko	University of Würzburg
Dr. Kai Gellert	University of Wuppertal
Prof. Dr. Ing. Bela Gipp	Universität Göttingen
Dr. Maximilian Golla	CISPA Helmholtz Center for Information Security
Prof. Dr. Matteo Große-Kampmann	Rhine-Waal University of Applied Sciences
Prof. Dominik Herrmann	Universität Bamberg
Prof. Dr. Matthias Hollick	TU Darmstadt
Prof. Ralph Holz	University of Münster
Prof. Thorsten Holz	CISPA Helmholtz Center for Information Security
Dr. Máté Horváth	University of Wuppertal

Dr. Catalin Hritcu	Max Planck Institute for Security and Privacy
Prof. Dr.-Ing. Tibor Jager	University of Wuppertal
Prof. Dr. Stefan Katzenbeisser	University of Passau
Prof. Dr.-Ing. Elif Bilge Kavun	University of Passau
Dr. Katharina Krombholz	CISPA Helmholtz Center for Information Security
Dr. Michael Kubach	Fraunhofer IAO
Prof. Anja Lehmann	Hasso-Plattner-Institute, University of Potsdam
Dr. Wouter Lueks	CISPA Helmholtz Center for Information Security
Prof. Esfandiar Mohammadi	University of Lübeck
Prof. Dr. Veelasha Moonsamy	Ruhr University Bochum
Prof. Dr.-Ing. Andreas Noack	Hochschule Stralsund
Prof. Dr. Lorenz Panny	TU Munich
Dr. Giancarlo Pellegrino	CISPA Helmholtz Center for Information Security
Florentin Putz	TU Darmstadt
Prof. Konrad Rieck	TU Berlin
Prof. Paul Rösler	FAU Erlangen-Nürnberg
Prof. Dr. Sebastian Schinzel	Münster University of Applied Sciences
Prof. Thomas Schneider	TU Darmstadt
Prof. Dr. Peter Schwabe	MPI-SP & Radboud University
Prof. Dr. Jörg Schwenk	Ruhr University Bochum
Dr. Lea Schönherr	CISPA Helmholtz Center for Information Security
Dr. Mridula Singh	CISPA Helmholtz Center for Information Security
Prof. Dr. Daniel Slamanig	Universität der Bundeswehr München
Dr.-Ing. Ben Stock	CISPA Helmholtz Center for Information Security
Prof. Dr. Thorsten Strufe	Karlsruher Institut für Technologie / TU Dresden
Dr. Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security
Dr.-Ing. Amos Treiber	Personal capacity

Dr. Anjo Vahldiek-Oberwagner	Intel Labs
Prof. Dr. Yuval Yarom	Ruhr University Bochum
Dr. Yixin Zou	Max Planck Institute for Security and Privacy

Greece

Prof. Stefanos Gritzalis	University of Piraeus
Prof. Christos Kalloniatis	University of the Aegean
Prof. Spyros Kokolakis	University of the Aegean
Prof. Costas Lambrinoudakis	University of Piraeus
Prof. Panagiotis Rizomiliotis	Harokopio University of Athens

Hong Kong SAR, China

Prof. Sherman S. M. Chow	Chinese University of Hong Kong

Iceland

Prof. Hans P. Reiser	Reykjavik University

Ireland

Dr. Stephen Farrell	Trinity College Dublin
Dr. TJ McIntyre	University College Dublin, Sutherland School of Law
Dr. Paolo Palmieri	University College Cork

Israel

Prof. Orr Dunkelman	University of Haifa
Dr. Eyal Ronen	Tel Aviv University
Dr. Mahmood Sharif	Tel Aviv University

Italy

Dr. Daniele Cono D'Elia	Sapienza University of Rome
Prof. Stefano Zanero	Politecnico di Milano

Japan

Prof. Takao Murakami	The Institute of Statistical Mathematics

Liechtenstein

Prof. Giovanni Apruzzese	University of Liechtenstein

Luxembourg

Prof. Peter Y A Ryan	University of Luxembourg

Norway

Prof. Dr. Lothar Fritsch	Oslo Metropolitan University
Dr. Erik Hjelmås	NTNU
Dr. Håvard Raddum	Simula UiB
Prof. Tjerand Silde	NTNU

Poland

Prof. Miroslaw Kutylowski	NASK

Portugal

Prof. Manuel Barbosa	University of Porto (FCUP) & INESC TEC & MPI SP
Prof. Nuno Santos	INESC-ID / Instituto Superior Técnico, University of Lisbon

Romania

Dr. George Teseleanu	Institute of Mathematics of the Romanian Academy

South Korea

Prof. Sang Kil Cha	KAIST
Yuseok Jeon	Ulsan National Institute of Science and Technology

Spain

Prof. Pino Caballero-Gil	Universidad de La Laguna
Prof. Josep Domingo-Ferrer	Universitat Rovira i Virgili
Prof. Jose Maria de Fuentes	Universidad Carlos III Madrid
Dr. Marco Guarnieri	IMDEA Software Institute
Prof. Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona
Prof. Lorena González Manzano	Universidad Carlos III Madrid
Prof. David Megías	Universitat Oberta de Catalunya
Dr. Pedro Moreno-Sanchez	IMDEA Software Institute
Prof. Gorka Guardiola Múzquiz	Universidad Rey Juan Carlos
Prof. Antonio Nappa	Universidad Carlos III Madrid
Dr. Sergio Pastrana	Univesidad Carlos III Madrid
Dr. Helena Rifà-Pous	Universitat Oberta de Catalunya
Prof. Dr. Ricardo J. Rodríguez	Universidad de Zaragoza
Prof. Enrique Soriano-Salvador	Universidad Rey Juan Carlos
Dr. Guillermo Suarez-Tangil	IMDEA Networks Institute
Prof. María Isabel González Vasco	Universidad Carlos III Madrid

Sweden

Dr. Mikael Asplund	Linköping University

Prof. Dr.-Ing. Meiko Jensen	Karlstad University
Dr. Leonardo Martucci	Karlstad University
Dr. Nurul Momen	Blekinge Institute of Technology
Prof. Panos Papadimitratos	KTH Royal Institute of Technology
Dr. Tobias Pulls	Karlstad University
Dr. Apostolos Pyrgelis	RISE Research Institutes of Sweden

Switzerland

Prof. Christian Cachin	University of Bern
Prof. Srdjan Capkun	ETH Zurich
Dr. Anastasija Collen	University of Geneva
Dr. Ana-Maria Cretu	EPFL
Prof. Jean-Pierre Hubaux	EPFL
Dr. Kari Kostiainen	ETH Zurich
Dr. Anil Kurmus	Personal capacity
Prof. Rebekah Overdorf	University of Lausanne
Prof. Mathias Payer	EPFL
Alessandro Sorniotti	IBM Research Europe
Prof. Dr. Florian Tramèr	ETH Zurich
Prof. Carmela Troncoso	EPFL

Taiwan

Dr. Matthias J. Kannwischer	Chelpis Quantum Tech

The Netherlands

Dr. Gunes Acar	Radboud University
Prof. Frederik Zuiderveen Borgesius	iHub, Radboud University

Prof. Herbert Bos	Vrije Universiteit Amsterdam
Dr. Andrea Continella	University of Twente
Prof. Dr. Ronald Cramer	CWI & Leiden University
Prof. Joan Daemen	Radboud University
Prof. Marten van Dijk	CWI
Prof. Dr. Jaap-Henk Hoepman	Radboud University / University of Groningen / Karlstad University
Prof. Dr. Bart Jacobs	Radboud University
Dr. Chenglu Jin	CWI Amsterdam
Dr. Karst Koymans	University of Amsterdam
Prof. Dr. Tanja Lange	Eindhoven University of Technology
Prof.Dr. Ronald Leenes	Tilburg University
Prof. Luca Mariot	University of Twente
Dr. Kostas Papagiannopoulos	University of Amsterdam
Prof. Dr. ir. Roland van Rijswijk-Deij	University of Twente
Dr. Simona Samardjiska	Radboud University
Prof. Dr. Christian Schaffner	University of Amsterdam
Dr. Jeroen van der Ham-de Vos	University of Twente

Turkey

Prof. Cihangir Tezcan	Middle East Technical University

United Arab Emirates

Prof. Michail Maniatakos	New York University Abu Dhabi
Prof. Christina Pöpper	New York University Abu Dhabi

United Kingdom

Dr. Ruba Abu-Salma	King's College London
Prof. Martin Albrecht	King's College London
Dr. Andrea Basso	University of Bristol
Prof. Ioana Boureanu	University of Surrey
Prof. Lorenzo Cavallaro	University College London
Dr. Giovanni Cherubin	Microsoft
Dr. Benjamin Dowling	University of Sheffield
Dr. François Dupressoir	University of Bristol
Dr. Jide Edu	University of Strathclyde
Dr. Arthur Gervais	University College London
Prof. Hamed Haddadi	Imperial College London
Prof. Alice Hutchings	University of Cambridge
Dr. Dennis Jackson	Mozilla
Dr. Rikke Bjerg Jensen	Royal Holloway University of London
Prof. Keith Martin	Royal Holloway University of London
Dr. Maryam Mehrnezhad	Royal Holloway University of London
Prof. Sarah Meiklejohn	University College London
Dr. Ngoc Khanh Nguyen	King's College London
Prof. Elisabeth Oswald	University of Birmingham
Dr. Daniel Page	University of Bristol
Dr. Eamonn Postlethwaite	King's College London
Dr. Kopo Marvin Ramokapane	University of Bristol
Prof. Awais Rashid	University of Bristol
Dr. Daniel R. Thomas	University of Strathclyde
Dr. Yiannis Tselekounis	Royal Holloway University of London
Dr. Michael Veale	University College London
Prof. Dr. Luca Viganò	King's College London

Dr. Petros Wallden	University of Edinburgh
Dr. Christian Weinert	Royal Holloway University of London

United States of America

Prof. Kendra Albert	Harvard University
Prof. Adam J. Aviv	The George Washington University
Prof. Lujo Bauer	Carnegie Mellon University
Prof. Joseph Bonneau	New York University
Prof. Varun Chandrasekaran	University of Illinois Urbana-Champaign
Prof. Rahul Chatterjee	University of Wisconsin-Madison
Dr. Camille Cobb	University of Illinois
Prof. Álvaro Cárdenas	UCSC
Prof. Sven Dietrich	City University of New York
Prof. Zakir Durumeric	Stanford University
Prof. Earlence Fernandes	UC San Diego
Dr. Gemma Galdon-Calvell	Eticas
Prof. Christina Garman	Purdue University
Dr. Matthew D. Green	Johns Hopkins University
Prof. Xiali Hei	University of Louisiana at Lafayette
Prof. Susan Landau	Tufts University
Prof. Zhiqiang Lin	Ohio State University
Prof. Michelle Mazurek	University of Maryland
Dr. Peter G. Neumann	SRI Computer Science Lab
Dr. Niels Provos	Lacework
Dr. Lucy Qin	Georgetown University
Prof. Sazzadur Rahaman	University of Arizona
Prof. Amir Rahmati	Stony Brook University

Prof. Elissa Redmiles	Georgetown University
Prof. Ronald L. Rivest	MIT
Prof. Nitesh Saxena	Texas A&M University
Dr. Sarah Scheffler	MIT
Prof. Bruce Schneier	Harvard Kennedy School
Prof. Micah Sherr	Georgetown University
Mr. Adam Shostack	University of Washington
Alin Tomescu	Aptos Labs
Prof. Blase Ur	University of Chicago
Dr. Dionysis Zindros	Stanford University

If you are a scientist or researcher and want to sign please fill out this form hosted by the Chaos Computer Club of Vienna (PhD or demonstrated research track record required).