

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

Signatures on 31 July @ 12pm

Signatories: 465

Countries: 38

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)

Eyal Ronen - eyal.ronen@cs.tau.ac.il (Israel)

TJ McIntyre - tjmcintyre@ucd.ie (Ireland)

Jaap-Henk Hoepman - jhh@cs.ru.nl (The Netherlands)

Aurelien Francillon - aurelien.francillon@eurecom.fr (France)

Anja Lehmann - anja.lehmann@hpi.de (Germany)

René Mayrhofer - rm@ins.jku.at (Austria)

Diego Aranha - dfaranha@cs.au.dk (Denmark)

Cihangir Tezcan - cihangir@metu.edu.tr (Turkey)

Mauro Conti - mauro.conti@unipd.it (Italy)

Stefan Dziembowski - stefan.dziembowski@gmail.com (Poland)

We continue the signature collection. If you are a scientist or researcher and would like to add your name please fill this form: <https://tinyurl.com/ResearchersCSA> (PhD or demonstrated research track record required)

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 proposed Child Sexual Abuse Regulation: 4 July 2023

The signatories of this statement are scientists and researchers from across the globe.

First and foremost, we acknowledge that child sexual abuse and exploitation is a very serious crime which can cause lifelong harm to survivors. It is the responsibility of government authorities, with the support of companies and communities, to undertake effective interventions which prevent this crime and react to it quickly when it does happen.

The European Commission has proposed a law with the stated aim of stopping the spread of child sexual abuse material online and of grooming of children online. To do so, the law allows authorities to compel providers of any apps or other online services to scan the messages, pictures, emails, voice mails and other activities of their users. In the case of end-to-end encrypted apps, the claim is that this scanning can be done on users' devices – so-called 'Client-Side Scanning' (CSS).

The effectiveness of the law (at its stated aims) relies on the existence of effective scanning technologies. Unfortunately, the scanning technologies that currently exist and that are on the horizon are deeply flawed. These flaws, which we describe in detail below, means that scanning is doomed to be ineffective. Moreover, integrating scanning at large scale on apps running in user devices, and particularly in a global context, creates side-effects that can be extremely harmful for everyone online, and which could make the Internet and the digital society less safe for everybody.

As the problems we describe speak to measures that are at the core of the EU's legislative proposal, it is our professional recommendation as scientists that such a proposal be not taken forward. It is not feasible or tenable to require private companies to use technologies in ways that we already know cannot be done safely – or even at all. Given the horrific nature of child sexual abuse, it is understandable, and indeed tempting, to hope that there is a technological intervention that can eradicate it. Yet, looking at the issue holistically, we cannot escape the conclusion that the current proposal is not such an intervention.

Passing this legislation undermines the thoughtful and incisive work that European researchers have provided in cybersecurity and privacy, including contributions to the development of global encryption standards. Such undermining will weaken the environment for security and privacy work in Europe, lowering our ability to build a secure digital society.

The proposed regulation would also set a global precedent for filtering the Internet, controlling who can access it, and taking away some of the few tools available for people to protect their right to a private life in the digital space. This will have a chilling effect on society and is likely to negatively affect democracies across the globe.

We therefore strongly warn against pursuing these or similar measures as their success is not possible given current and foreseeable technology, while their potential for harm is substantial.

1. Detection technologies are deeply flawed and vulnerable to attacks

Tools used for scanning for **known Child Sexual Abuse Material (CSAM)** must not contain CSAM material itself as this would bring major risks. Thus, the only scalable technology to address this problem is by transforming the known content with a so-called perceptual hash function and by using a list of the resulting hash values to compare to potential CSAM material. A perceptual hash function needs to achieve two goals: (i) it should be easy to compute yet hard to invert and (ii) small changes to an image should result in small changes to the hash output, which means that even after image manipulation the known image can still be detected. While this sounds easy, after more than two decades of research there has been no substantial progress in designing functions that meet these properties.

Research has shown that for all known perceptual hash functions, it is virtually always possible to make small changes to an image that result in a large change of the hash value which allows evasion of detection (false negative). Moreover, it is also possible to create a legitimate picture that will be falsely detected as illegal material as it has the same hash as a picture that is in the database (false positive). This can be achieved even without knowing the hash database. Such an attack could be used to frame innocent users and to flood Law Enforcement Agencies with false positives – diverting resources away from real investigations into child sexual abuse.

These attacks are not theoretical: for concrete designs such as Photo DNA, Facebook's PDQ hash function and Apple's NeuralHash function, efficient attacks have been described in the literature. The only way to avoid such attacks for the time being is by keeping the description of the perceptual hash function secret. This "security by obscurity" not only goes against basic security engineering principles but, in practice, is only feasible if the perceptual hash function is known only to the service provider. In the case of end-to-end encryption, the hashing operation needs to take place on the client device. Thus, keeping the design secret is an illusion.

As scientists, we do not expect that it will be feasible in the next 10-20 years to develop a scalable solution that can run on users' devices without leaking illegal information and that can detect known content (or content derived from or related to known content) in a reliable way, that is, with an acceptable number of false positives and negatives.

The proposal of the European Commission goes beyond the detection of known content. It also requires that **newly generated images or videos** with CSAM need to be detected based on "artificial intelligence" tools. In addition, the proposal requires that **grooming in communication services** including both text and audio should be detected using similar techniques. While some commercial players claim that they have made progress, the designs remain secret and no open and objective evaluation has taken place that demonstrates their effectiveness. Moreover, the state of the art in machine learning suggests that this is way beyond what is feasible today. In fact, any time that client-side designs have been evaluated (as in the case of prototypes funded by the UK Home office) they have been found to be neither effective nor compliant with privacy and human-rights law.

AI tools can be trained to identify certain patterns with high levels of precision. However, they routinely make errors, including mistakes that to a human seem very basic. That is because AI systems lack context and common sense. There are some tasks to which AI systems are

well-suited, but searching for a very nuanced, sensitive crime — which is what grooming behaviour is — is not one of these tasks.

At the scale at which private communications are exchanged online, even scanning the messages exchanged in the EU on just one app provider would mean generating millions of errors every day. That means that when scanning billions of images, videos, texts and audio messages per day, the number of false positives will be in the hundreds of millions. It further seems likely that many of these false positives will themselves be deeply private, likely intimate, and entirely legal imagery sent between consenting adults.

This cannot be improved through innovation: ‘false positives’ (content that is wrongly flagged as being unlawful material) are a statistical certainty when it comes to AI. False positives are also an inevitability when it comes to the use of detection technologies -- even for known CSAM material. The only way to reduce this to an acceptable margin of error would be to only scan in narrow and *genuinely* targeted circumstances where there is prior suspicion, as well as sufficient human resources to deal with the false positives -- otherwise cost may be prohibitive given the large number of people who will be needed to review millions of texts and images. This is not what is envisioned by the European Commission’s proposal.

The reporting system put forward in the draft CSAM proposal is likely to encourage novel attacks on detection technologies. This is because right now, providers have the discretion to sift out obvious false alerts. Under the new system, however, they would be required to report even content that seems unlikely to be CSAM. Besides the attacks we mention, many more are starting to appear in specialized academic venues, and we expect many more are being prepared by those motivated to share illicit material.

Finally, it has been claimed that detecting CSAM should be feasible as scanning for computer viruses is a widely deployed technology. While superficially both seem similar, there are essential differences. First, when a computer virus is detected, the user is warned and the virus can be removed. Second, a virus can be recognized based on a small unique substring, which is not the case for a picture or video: it would be very easy to modify or remove a unique substring with small changes that do not change the appearance; doing this for a virus would make the code inoperable. Finally, machine learning techniques can sometimes identify viral behaviour, but only when such behaviour can be precisely defined (e.g. code that copies itself) and thus detected. This is in opposition to defining CSAM for which clear boundaries cannot easily be established.

2. Technical Implications of weakening End-to-End Encryption

End-to-end encryption is designed so that only the sender and recipient can view the content of a message or other communication. Encryption is the only tool we have to protect our data in the digital realm; all other tools have been proven to be compromised. The use of link encryption (from user to service provider and from service provider to user) with decryption in the middle as used in the mobile telephone system is not an acceptable solution in the current threat environment. It is obvious that end-to-end encryption makes it impossible to implement scanning for known or new content and detection of grooming at the service provider.

In order to remedy this, a set of techniques called “Client-Side Scanning” (CSS) has been suggested as a way to access encrypted communications without breaking the encryption. Such tools would reportedly work by scanning content on the user’s device before it has been encrypted or after it has been decrypted, then reporting whenever illicit material is found. One may equate this to adding video cameras in our homes to listen to every conversation and send reports when we talk about illicit topics.

The only deployment of CSS in the free world was by Apple in 2021, which they claimed was state-of-the-art technology. This effort was withdrawn after less than two weeks due to privacy concerns and the fact that the system had already been hijacked and manipulated.

When deployed on a person’s device, CSS acts like spyware, allowing adversaries to gain easy access to that device. Any law which would mandate CSS, or any other technology designed to access, analyse or share the content of communications will, without a doubt, undermine encryption, and make everyone’s communications less safe as a result. The laudable aim of protecting children does not change this technical reality.

Even if such a CSS system could be conceived, there is an extremely high risk that it will be abused. We expect that there will be substantial pressure on policymakers to extend the scope, first to detect terrorist recruitment, then other criminal activity, then dissident speech. For instance, it would be sufficient for less democratic governments to extend the database of hash values that typically correspond to known CSAM content (as explained above) with hash values of content critical of the regime. As the hash values give no information on the content itself, it would be impossible for outsiders to detect this abuse. The CSS infrastructure could then be used to report all users with this content immediately to these governments.

If such a mechanism would be implemented, it would need to be in part through security by obscurity as otherwise it would be easy for users to bypass the detection mechanisms, for example by emptying the database of hash values or bypassing some verifications. This means that transparency of the application will be harmed, which may be used by some actors as a veil to collect more personal user data.

3. Effectiveness

We have serious reservations whether the technologies imposed by the regulation would be effective: perpetrators would be aware of such technologies and would move to new techniques, services and platforms to exchange CSAM information while evading detection.

The proposed regulation will harm the freedom of children to express themselves as their conversations could also be triggering alarms. National criminal law enforcement on-the-ground typically deals in a nuanced way with intimate messages between teenagers both around the age of consent. These technologies change the relationship between individuals and their devices, and it will be difficult to reintroduce such nuance. For other users, we have major concerns of the chilling effects created by the presence of these detection mechanisms.

Finally, the huge number of false positives that can be expected will require a substantial amount of resources while creating serious risks for all users to be identified incorrectly. These resources would be better spent on other approaches to protect children from sexual abuse. While most child protection work must be local, one way in which community legislation might help is by using existing powers (DMA/DSA) to require social network services to make it easier for users to complain about abuse, as it is user complaints rather than AI that in practice lead to the detection of new abuse material.

Signed,

Australia

Dr. Shaanan Cohney	University of Melbourne
Prof. Vanessa Teague	Australian National University & Thinking Cybersecurity Pty Ltd

Austria

Prof. Dr. Elena Andreeva	TU Wien
Univ.-Prof. Dr. Rainer Böhme	Universität Innsbruck
Dr. Gaëtan Cassiers	TU Graz
Prof. Maria Eichlseder	TU Graz
Prof. Daniel Gruss	TU Graz
Dr. Stephan Krenn	Personal capacity
Prof. Dr. Martina Lindorfer	TU Wien
Univ.-Prof. Dr. Matteo Maffei	TU Wien
Prof. Stefan Mangard	TU Graz
Univ.-Prof. Dr. René Mayrhofer	Johannes Kepler University Linz
Prof. Elisabeth Oswald	University of Klagenfurt
Dr. Erich Prem	University of Vienna
Univ.-Prof. Dr. Christian Rechberger	TU Graz
Dr. Michael Roland	Johannes Kepler University Linz
Univ.-Prof. Edgar Weippl	University of Vienna, SBA Research

Belgium

Dr. Ir. Aysajan Abidin	KU Leuven	
Dr. Nicholas Bleisch	KU Leuven	
Prof. Dr. Rosamunde van Brakel	Vrije Universiteit Brussel	
Prof. Claudia Diaz	KU Leuven	
Dr. Benedikt Gierlichs	KU Leuven	
Prof. Dr. Gloria González Fuster	Vrije Universiteit Brussel	
Dr. Emad Heydari Beni	KU Leuven	
Prof. Dr. Joris van Hoboken	University of Amsterdam and Vrije Universiteit Brussel	
Prof. Jan Tobias Muehlberg	Universite Libre de Bruxelles	
Dr. Thorben Moos	UCLouvain	
Prof. Yves Moreau	KU Leuven	
Dr. Vera Rimmer	KU Leuven	
Prof. Olivier Pereira	UCLouvain	
Prof. Thomas Peters	UCLouvain	
Prof. Bart Preneel	KU Leuven	Fellow IACR
Prof. Dr. Frederik Questier	Vrije Universiteit Brussel	
Prof. Em. Jean-Jacques Quisquater	UC Louvain	
Prof. Florentin Rochet	University of Namur	
Prof. Nigel Smart	KU Leuven	Fellow IACR
Prof. François-Xavier Standaert	UCLouvain	
Prof. Mathy Vanhoef	KU Leuven	
Prof. Ingrid Verbauwhede	KU Leuven	Fellow IACR, IEEE

Brazil

Mr. Carlos A. Afonso	Instituto Nupef & ISOC-Brazil
Prof. Ian Brown	Centre for Technology & Society, Fundação Getulio Vargas
Prof. Alexandre Augusto Giron	Federal University of Technology - Parana
Dr. Jean Martina	Universidade Federal de Santa Catarina
Prof. Dr. Marcos Antonio Simplicio Jr	Universidade de Sao Paulo

Bulgaria

Dr. Konstantin Delchev	Institute of Mathematics and Informatics and Bulgarian Academy of Sciences
------------------------	---

Canada

Prof. Ron Deibert	Citizen Lab at the University of Toronto
Prof. Ian Goldberg	University of Waterloo
Prof. Florian Kerschbaum	University of Waterloo
Prof. David Lie	University of Toronto
Dr. Simón Oya	University of Waterloo
Prof. Nicolas Papernot	University of Toronto and Vector Institute
	Canada Research Chair Fellow Sloan

Chile

Prof. Alejandro Hevia	University of Chile
-----------------------	---------------------

Czechia

Dr. Vit Bukac	Masaryk University
Prof. Vashek Matyas	Masaryk University
Dr. Kamil Malinka	Brno University of Technology
Dr. Petr Svenda	Masaryk University
Dr.. Marek Sys	Masaryk University
Dr. Martin Ukrop	Masaryk University

Denmark

Prof. Diego F. Aranha	Aarhus University
Prof. Dimitrios Askitis	University of Copenhagen
Prof. Carsten Baum	Technical University of Denmark
Prof. Joan Boyar	University of Southern Denmark
Prof. Ivan Damgård	Aarhus University
Prof. Bernardo David	University of Copenhagen
Dr. Christian Majenz	Technical University of Denmark
Prof. Claudio Orlandi	Aarhus University
Prof. Luisa Siniscalchi	Technical University Denmark
Prof. Peter Scholl	Aarhus University
Prof. Tyge Tiessen	Technical University Denmark
Prof. Dr. Emmanouil Vasilomanolakis	Technical University Denmark
	Fellow IACR

Estonia

Dr. Dan Bogdanov	Personal capacity	Estonian Academy of Sciences
------------------	-------------------	------------------------------

Finland

Prof. Antti Honkela	University of Helsinki
Prof. Kimmo Halunen	University of Oulu

France

Dr. Daniele Antonioli	EURECOM
Dr. Daniel Augot	Inria
Dr. Gustavo Banegas	Independent Researcher
Dr. Benjamin Beurdouche	Mozilla
Mr. Karthikeyan Bhargavan	Cryspen
Dr. Bruno Blanchet	Inria
Prof. Olivier Blazy	École Polytechnique
Prof. Christina Boura	University of Versailles
Dr. Anne Canteaut	Inria

Dr. Em. Pascale Charpin
 Dr. Veronique Cortier
 Dr. Jannik Dreier
 Prof. Antonio Faonio
 Dr. Caroline Fontaine
 Dr. Aurélien Francillon
 Dr. Aymeric Fromherz
 Dr. Pierrick Gaudry
 Prof. Elham Kashefi
 Dr. Jonathan Keller
 Dr. Nadim Kobeissi
 Dr. Steve Kremer
 Dr. Gaëtan Leurent
 Dr. Pierre Laperdrix
 Dr. Victor Lomné
 Dr. P. G. Macioti
 Dr. Clémentine Maurice
 Hon. Dr. Traian Muntean
 Prof. Melek Önen
 Dr. Maria Naya Plasencia
 Dir. Research Catuscia Palamidessi
 Dr. Léo Perrin
 Dr. Peter Roenne
 Dr. Yann Rote
 Dr. Emmanuel Thomé
 Dr. Anna Weine

Inria
 CNRS
 Université de Lorraine
 EURECOM
 CNRS
 EURECOM
 Inria
 CNRS
 CNRS and University of Edimburgh
 Institut Mines Telecom
 Symbolic Software
 Inria
 Inria
 CNRS
 NinjaLab
 Medicines du Monde
 CNRS
 Aix-Marseille University
 EURECOM
 Inria
 Inria
 Inria
 CNRS
 Université Paris-Saclay
 Inria
 Mozilla

Germany

Dr. Ali Abassi
 Prof. Patricia Arias Cabarcos
 Prof. Dr. Alexander Auch
 Dr. Gilles Barthe
 Dr. Steffen Becker

 Prof. Dr. Bettina Berendt
 Dr. Sebastian Berndt
 Dr. Asia Biega
 Dr. Christopher Blöcker
 Dr. Marcel Böhme
 Dr. Harald Böhme
 Prof. Dr. Kevin Borgolte
 Dr. Sven Bugiel
 Dr. Rebekka Burkholz
 Dr.-Ing. Jiska Classen
 Prof. Dr. Cas Cremers
 Prof. Dr.-Ing. Alexandra Dmitrienko
 Prof. Thomas Eisenbarth
 Prof. Sebastian Faust
 Dr.-Ing. Daniel Demmler
 Dr. Christian Gollwitzer
 Dr. Dominik Helm
 Prof. Dr. Jeanette Hofmann
 Prof. Thorsten Holz
 Prof. Matthias Hollick
 Dr. Julian Hoth
 Prof. Tibor Jäger
 Prof. Dr. Stefan Katzenbeisser
 Dr. Dietmar Kammerer
 Dr. Elif Bilge Kavun
 Dr. Franziskus Kiefer

CISA Helmholtz Center for Information Security
 Paderborn University
 Baden-Wuerttemberg Cooperative State University
 Max Planck Institute for Security and Privacy
 Ruhr University Bochum &
 Max Planck Institute for Security and Privacy
 TU Berlin and KU Leuven
 University of Lübeck
 Max Planck Institute for Security and Privacy
 Julius-Maximilians-Universität Würzburg
 Max Planck Institute for Security and Privacy
 ANSYS Germany
 Ruhr University Bochum
 CISA Helmholtz Center for Information Security
 CISA Helmholtz Center for Information Security
 Hasso Plattner Institute
 CISA Helmholtz Center for Information Security
 Julius-Maximilians Universität Würzburg
 University of Lübeck
 Technical University of Darmstadt
 Personal Capacity
 Physikalisch-Technische Bundesanstalt
 Technische Universität Darmstadt
 Berlin Social Science Center
 CISA Helmholtz Center for Information Security
 Technical University of Darmstadt
 Hamburg University of Technology
 University of Wuppertal
 University of Passau
 Weizenbaum Institute for the Networked Society
 University of Passau
 Cryspen

Prof. Dr. phil Thomas Knaus
 Dr. Katharina Krombholz
 Prof. Anja Lehmann
 Dr. Ferdinand Lehmann
 Prof. Dr. Daniel Loebenberger
 Dr. Alexander Loew
 Dr. Wouter Lueks
 Dr. Genia Lücking
 Dr. Thomas Mager
 Dr. Christian Mainka
 Dr. Jens Meier
 Prof. Dr. Esfandiar Mohammadi
 Dr. Veelasha Moonsamy
 Prof. Dr. Andreas Peter
 Dr. Giancarlo Pellegrino
 Dr. Henrich C. Pöhls
 Prof. Joachim Posegga
 Prof. Dr. Kai Rannenber
 Dr. Elissa Redmiles
 Dipl. Inf. Rainer Rehak
 Prof. Konrad Rieck
 Prof. Stefanie Roos
 Prof. Paul Rösler
 Prof. Dr. Christian Rossow
 Prof. Dr. Christoph Skornia
 Dr. Jens Schade
 Prof. Dr. Sebastian Schinzel
 Prof. Thomas Schneider
 Prof. Dr. Marc C. Steinbach
 Prof. Dr. Dominique Schröder
 Dr. Peter Schwabe
 Dipl. Ir. Peter Schoo
 Prof. Dr. Ingo Scholtes
 Prof. Juraj Somorovsky
 Prof. Dr. Christoph Sorge
 Dr. Ben Stock
 Prof. Thorsten Strufe

Prof. Florian Tschorsch
 Dr. Nils Ole Tippenhauer
 Dr. Anjo Vahldiek-Oberwagner
 Dr. Vera Wilde
 Prof. Christian Wressnegger
 Prof. Dr. Yuval Yarom
 Dr. Xiao Zhang
 Dr. Yixin Zou

Greece

Prof. Vasiliki Diamantopoulou
 Prof. Christos Kalloniatis
 Prof. Georgios Kambourakis
 Dr. Platon Kotzias
 Prof. Costas Lambrinoudakis
 Prof. Emmanouil Magkos
 Prof. Stefanos Gritzalis

Prof. Panagiotis Rizomiliotis

Hungary

PH Ludwigsburg | FTzM Frankfurt/Main
 CISPA Helmholtz Center for Information Security
 Hasso-Plattner-Institute, University of Potsdam
 Justus Liebig Universität Gießen
 Fraunhofer AISEC / OTH Amberg-Weiden
 DWH
 CISPA Helmholtz Center for Information Security
 Technical University of Munich
 Personal capacity
 Ruhr University Bochum
 Deutsches Institut für Kautschuktechnologie e.V.
 University of Lübeck
 Ruhr University Bochum
 University of Oldenburg
 CISPA Helmholtz Center for Information Security
 University of Passau
 University of Passau
 Goethe University Frankfurt
 Max Planck Institute for Software Systems
 Weizenbaum Institute for the Networked Society
 Technische Universität Berlin
 University of Kaiserslautern-Landau
 FAU Erlangen-Nürnberg
 CISPA Helmholtz Center for Information Security
 University of Applied Sciences Regensburg
 TU Dresden
 Münster University of Applied Sciences
 Technische Universität Darmstadt
 Leibniz Universität Hannover
 Friedrich-Alexander Universität Erlangen-Nürnberg
 Max Planck Institute for Security and Privacy
 Personal Capacity Fellow ACM
 Julius-Maximilians-Universität Würzburg
 Paderborn University
 Saarland University
 CISPA Helmholtz Center for Information Security
 KASTEL/Karlsruhe &
 Centre for Tactile Internet with Human-in-the-Loop, Dresden
 TU Berlin and HU Berlin
 CISPA Helmholtz Center for Information Security
 Intel Labs
 Freelance
 Karlsruhe Institute of Technology
 Ruhr University Bochum
 CISPA Helmholtz Center for Information Security
 Max Planck Institute for Security and Privacy

University of the Aegean
 University of the Aegean
 University of the Aegean
 Norton Research Group
 University of Piraeus
 Ionian University
 University of Piraeus and
 Hellenic Authority for Communication Security and Privacy
 Harokopio University of Athens

Dr. Gergely Biczók
Dr. Balazs Pejo

Budapest Univ. of Technology and Economics
Budapest Univ. of Technology and Economics

Ireland

Dr. Stephen Farrell
Dr. Aikaterini Kanta
Prof. Douglas Leith
Dr. TJ McIntyre

Trinity College Dublin
University College Dublin
Trinity College Dublin
University College Dublin Sutherland School of Law &
Digital Rights Ireland
Irish Council for Civil Liberties

Dr. Kris Shrishak

India

Dr. Chaya Ganesh

Indian Institute of Science

Israel

Prof. Orr Dunlekman
Dr. Yossi Oren
Dr. Eyal Ronen
Dr. Mahmood Sharif

University of Haifa
Ben-Gurion University
Tel Aviv University
Tel Aviv University

Italy

Prof. Stefano Calzavara
Prof. Mauro Conti
Prof. Bruno Crispo
Prof. Paolo Falcarin
Prof. Fabio Massaci
Dr. Daniela Morpurgo
Prof. Giuseppe Persiano
Dr. Dario Stabili
Prof. Daniele Venturi
Prof. Stefano Zanero

Università Ca' Foscari Venezia
University of Padua
University of Trento
University of Venice
University of Trento/Vrije Universiteit Amsterdam
Politecnico di Torino
Università di Salerno
University of Bologna
Sapienza University of Rome
Politecnico di Milano

Japan

Prof. Em. Toshimaru Ogura
Prof. Takao Murakami
Prof. Kazue Sako

Toyama University
The Institute of Statistical Mathematics (ISM)
Waseda University

Liechtenstein

Prof. Giovanni Apruzzese

University of Liechtenstein

Luxembourg

Dr. Orham Ermis
Dr. Aditya Damodaran
Prof. Dr. Gabriele Lenzini
Prof. Peter Y A Ryan

Luxembourg Institute of Science and Technology
University of Luxembourg
University of Luxembourg
University of Luxembourg

Mexico

Prof. Alejandro Pisanty

Universidad Nacional Autónoma de México

The Netherlands

Dr. Gunes Acar
Prof. Dr. Lejla Batina
Prof. Dr. LLM Frederik Z. Borgesius
Prof. Dr. ir. Herbert Bos
Dr. Corinne Cath
Dr. Andrea Continella
Prof. Ronald Cramer
Dr. Lorenzo Dalla Corte
Prof. Joan Daemen

Radboud University Nijmegen
Radboud University Nijmegen
iHub, Radboud University
Vrije Universiteit Amsterdam
Delft University of Technology
University of Twente
CWI & Leiden University
Tilburg University
Radboud University Nijmegen

Prof. Dr. Arie van Deursen
Dr. Ir. Roel Dobbe
Dr. Zekeriya Erkin
Prof. Cristiano Giuffrida
Dr. Seda Gürses
Dr. Florian Hahn
Prof. Jaap-Henk Hoepman
Prof. Andreas Hülsing
Dr. Georgy Ishmaev
Prof. Bart Jacobs
Dr. Konrad Kollnig
Dr. Matthijs Koot
Dr. Ralph Koning
Prof. Eleni Kosta
Prof. Dr. Tanja Lange
Dr. Luca Mariot
Dr. Giovane Moura
Dr. Laurens Naudts
Dr. Fatih Turkmen
Prof. Georgios Smaragdakis
Dr. Kitty Smeekes
Prof. Ot van Daalen
Prof. Michel van Eeten
Dr. Jeroen van der Ham
Prof. dr. Ir. Roland van Rijswijk-Deij
Dr. Heloise Vieira
Prof. Ben Wagner

Delft University of Technology
Delft University of Technology
Delft University of Technology
Vrije Universiteit Amsterdam
Delft University of Technology
University of Twente
Radboud University Nijmegen
Eindhoven University of Technology
Delft University of Technology
Radboud University Nijmegen
Maastricht University
University of Amsterdam & Secura BV
University of Amsterdam
Tilburg University
Eindhoven University of Technology
University of Twente
Delft University of Technology
University of Amsterdam
University of Groningen
Delft University of Technology
Personal capacity
University of Amsterdam
Delft University of Technology
University of Twente
University of Twente
Eindhoven University of Technology
Delft University of Technology

New Zealand

Prof. Brian E. Carpenter
Prof. Steven Galbraith

University of Auckland
University of Auckland

Norway

Prof. Anamaria Costache
Prof. Danilo Gligoroski
Dr. Erik Hjelmås
Prof. Helger Lipmaa
Prof. Sokratis Katsikas
Prof. Paweł Morawiecki
Dr. Vinit Ravishankar
Prof. David Palma
Prof. Tjerand Silde
Prof. Mohsen Toorani
Prof. Øyvind Ytrehus
Prof. Thomas Zinner

Norwegian University of Science and Technology
Norwegian University of Science and Technology
Norwegian University of Science and Technology
Simula UiB
Norwegian University of Science and Technology
Polish Academy of Sciences
University of Oslo
Norwegian University of Science and Technology
Norwegian University of Science and Technology
University of South-Eastern Norway
Simula UiB and University of Bergen
Norwegian University of Science and Technology

Poland

Prof. Stefan Dziembowski
Prof. Wojciech Jamroga
Dr. Dariusz Kalociński
Dr. Anna Ratecka

University of Warsaw
Institute of Computer Science, Polish Academy of Sciences
Institute of Computer Science, Polish Academy of Sciences
Jagiellonian University in Krakow

Portugal

Ms. Sofia Celi
Prof. Manuel Eduardo Correia
Prof. Manuel Barbosa
Prof. Hugo Pacheco
Prof. Bernardo Portela
Prof. Henrique Santos

Brave
University of Porto
University of Porto and INESC TEC
University of Porto
University of Porto
Universidade do Minho

Prof. Nuno Santos

INESC-ID and University of Lisbon

Republic of North Macedonia

Hristina Mihajloska Trpcheska

Ss. Cyril and Methodius University

Singapore

Prof. Thomas Peyrin

Nanyang Technological University

South Korea

Prof. Sang Kil Cha

KAIST

Spain

Dr. Jorge Blasco Alis

Prof. Pino Caballero-Gil

Dr. Ignacio Cascudo

Prof. Josep Domingo-Ferrer

Dr. Dario Fiore

Prof. Jose Maria de Fuentes

Dr. Gemma Galdon Clavell

Prof. Maribel González Vasco

Prof. Lorena González Manzano

Dr. Marco Guarnieri

Prof. Simona Levi

Dr. Jordi Herrera-Joancomartí

Prof. Llorenç Huguet

Dr. Guillermo Navarro-Arribas

Prof. Fernando Pérez-González

Dr. Cristina Perez-Sola

Dr. Helena Rifà-Pous

Dr. Guillermo Suarez-Tangil

Prof. Jose Such

Dr. Carla Ràfols

Prof. Josep Rifà

Prof. Juan Tapiador

Dr. Narseo Vallina-Rodriguez

Universidad Politécnica de Madrid

University of La Laguna

IMDEA Software Institute

Universitat Rovira i Virgili

IMDEA Software Institute

Universidad Carlos III de Madrid

Eticas Tech

Universidad Carlos III de Madrid

Universidad Carlos III de Madrid

IMDEA Software Institute

Xnet and University of Barcelona

Universitat Autònoma de Barcelona

Balearic Island University

Universitat Autònoma de Barcelona

University of Vigo

Universitat Autònoma de Barcelona

Universitat Oberta de Catalunya

IMDEA Networks Institute

Universitat Politècnica de Valencia

Universitat Pompeu Fabra

Universitat Autònoma de Barcelona

Universidad Carlos III de Madrid

IMDEA Networks Institute

Fellow IEEE

Fellow IEEE

Sweden

Prof. Simone Fischer-Hübner

Prof. Dr.-Ing. Meiko Jensen

Dr. Victor Morel

Prof. Panos Papadimitratos

Dr. Pablo Picazo-Sanchez

Dr. Tobias Pulls

Dr. Iraklis Symeonidis

Prof. Vicenç Torra

Karlstad University & Chalmers University of Technology

Karlstad University

Chalmers University

KTH Royal Institute of Technology

Halmstad University

Karlstad University

RISE

Umeå University

Fellow IEEE

Fellow IEEE

Switzerland

Dr. Anthony Boulmier

Dr. Jonathan Bootle

Prof. Srdjan Capkun

Prof. Bryan Ford

Dr. Jens Groth

Dr. Julia Hesse

Prof. Jean-Pierre Hubaux

Dr. Kari Kostianen

Dr. Anil Kurmus

Dr. Siniša Matetić

Prof. Marc Langheinrich

OptumSoft Inc.

Personal capacity

ETH Zurich

EPFL

DFINITY

IBM Zurich

EPFL

ETH Zurich

Personal Capacity

ETH Zurich

Università della Svizzera italiana

Fellow IEEE

Fellow ACM

Dr. Onicio Batista Leal Neto
 Prof. Rebekah Overdorf
 Prof. Kenneth Paterson
 Prof. Mathias Payer
 Dr Ivan Puddu
 Dr. Apostolos Pyrgelis
 Prof. Kaveh Razavi
 Dr. Raphael M. Reischuk
 Dr. Benjamin Rothenberger
 Dr. Alessandro Sorniotti
 Prof. Shweta Shinde
 Prof. Dr. Florian Tramèr
 Prof. Carmela Troncoso

ETH Zurich
 University of Lausanne
 ETH Zurich Fellow IACR
 EPFL
 ETH Zurich
 EPFL
 ETH Zurich
 National Test Institute for Cybersecurity NTC
 Zühlke Engineering AG
 Personal capacity
 ETH Zurich
 ETH Zurich
 EPFL

Taiwan

Dr. Lorenz Panny

Academia Sinica

Turkey

Prof. Mehmet Tahir Sandikkaya
 Prof. Cihangir Tezcan

Istanbul Technical University
 Middle East Technical University

United Arab Emirates

Prof. Michail Maniatakos
 Dr. Victor Mateu
 Prof. Chirstina Pöpper

New York University Abu Dhabi
 Technology and Innovation Institute
 New York University Abu Dhabi

United Kingdom

Dr. Ruba Abu-Salma
 Prof. Martin Albrecht
 Dr. Panagiotis Andriotis
 Prof. Ross Anderson
 Dr. Andrea Basso
 Dr. Pascal Berrang
 Prof. Alastair Beresford
 Prof. Reuben Binns
 Prof. Ioana Boureanu
 Dr. Jaya Klara Brekke
 Prof. Lorenzo Cavallaro
 Dr. Michele Ciampi
 Dr. George Chalhoub
 Prof. Liqun Chen
 Dr. Richard Clayton
 Dr. Kovila Coopamootoo
 Prof. Angela Daly
 Dr. Partha Das Chowdhury
 Dr. Santanu Dash
 Dr. Benjamin Dowling
 Dr. François Dupressoir
 Dr. Tariq Elahi
 Dr. Pooya Farshim
 Prof. Hamed Haddadi
 Prof. Julio Hernandez-Castro
 Dr. Alice Hutchings
 Dr. Martin Husovec
 Dr. Dennis Jackson
 Dr. Rikke Jensen
 Dr. Vitor Jesus
 Prof. Adam Joinson
 Dr. Philipp Jovanovic

King's College London
 King's College London
 University of Birmingham
 Universities of Cambridge and Edinburgh
 University of Bristol
 University of Birmingham
 University of Cambridge
 University of Oxford
 University of Surrey
 Nym Technologies
 University College London
 University of Edinburgh
 University of Oxford
 University of Surrey
 University of Cambridge
 King's College London
 University of Dundee
 University of Bristol
 Royal Holloway, University of London
 University of Sheffield
 University of Bristol
 University of Edinburgh
 Durham University
 Imperial College London
 University of Kent
 University of Cambridge
 London School of Economics and Political Science
 Mozilla
 Royal Holloway, University of London
 Aston University
 University of Bath
 University College London

Prof. Vasilis Katos
 Prof. Markulf Kohlweiss
 Dr. Kopo Marvin Ramokapane
 Prof. Aggelos Kiayias
 Dr. Bernardo Magri
 Prof. Corinne May-Chahal
 Prof. Keith Martin
 Dr. Maryam Mehrnezhad
 Prof. Sarah Meiklejohn
 Prof. Steven Murdoch
 Prof. Douwe Korff
 Dr. Daniel Page
 Dr. Claudia Peersman
 Prof. Andy Phippen
 Dr. Fabio Pierazzi
 Prof. Awais Rachid
 Dr. Luc Rocher
 Dr. Kaspar Rosager Ludvigsen
 Dr. Christos Sagredos
 Dr. Siamak Shahandashti
 Prof. Tom Stoneham
 Dr. Jose Tomas Llanos
 Dr. Michael Veale
 Dr. Niovi Vavoula
 Dr. Christian Weinert
 Prof. Alan Woodward
 Dr. Joss Wright

Bournemouth University
 University of Efinburgh
 University of Bristol
 University of Edinburgh
 University of Manchester
 University of Lancaster
 Royal Holloway, University of London
 Royal Holloway, University of London
 University College London
 University College London
 London Metropolitan University
 University of Bristol
 University of Bristol
 Bournemouth Universiy
 King's College London
 University of Bristol
 University of Oxford
 University of Edinburgh
 King's College London
 University of York
 University of York
 University College London
 University College London
 Queen Mary University of London
 Royal Holloway, University of London
 University of Surrey
 University of Oxford

United States of America

Prof. Giuseppe Ateniese
 Prof. Adam J. Aviv
 Prof. Steven Bellovin
 Prof. Matt Blaze
 Prof. Kevin Butler
 Mr. Jon Callas
 Prof. Álvaro Cárdenas
 Prof. Chandrasekaran
 Prof. David Choffnes
 Prof. Nicolas Christin
 Mr. Roger Dingledine
 Prof. Tudor Dumitras
 Prof. Zakir Durumeric
 Prof. Joan Feigenbaum
 Prof. Michael J. Fischer
 Dr. Kelsey Fulton
 Dr. Simson L. Garfinkel
 Prof. Christina Garman
 Prof. Matthew D. Green
 Prof. Daniel Genkin
 Prof. Paul Grubbs
 Dr. Joseph Lorenzo Hall
 Dr. Britta Hale
 Prof. Emeritus Martin Hellman
 Prof. Nadia Heninger
 Prof. Amir Herzberg
 Prof. Peter Honeyman
 Prof. Nicholas Hopper
 Prof. Gabriel Kaptchuk
 Prof. Vasileios Kemerlis
 Dr. Jennifer King

George Mason University
 George Washington University
 Columbia University
 Georgetown University McDevitt Chair of CS and Law
 University of Florida
 Personal capacity
 University of California, Santa Cruz
 University Illinois Urbana-Champaign
 Northeastern University
 Carnegie Mellon University
 The Tor Project
 University of Maryland
 Stanford University
 Yale University ACM Fellow
 Yale University ACM Fellow
 Colorado School of Mines
 Digital Corpora Project Fellow AAAS, ACM, IEEE
 Purdue University
 Johns Hopkins University
 Georgia Tech
 University of Michigan
 Internet Society
 Independent researcher
 Stanford University Turing Award
 University of California, San Diego
 University of Connecticut
 University of Michigan
 University of Minnesota
 Boston University
 Brown University
 Stanford University

Prof. Engin Kirda	Northeastern University	
Prof. Susan Landau	Tufts University	Fellow AAAS, ACM
Prof. Anna Lysyanskaya	Brown University	
Prof. Abigail Marsh	Macalester College	
Prof. David Mazières	Stanford University	
Prof. Michelle Mazurek	University of Maryland	
Prof. Ian Miers	University of Maryland	
Prof. Prateek Mittal	Princeton University	
Prof. Guevara Noubir	Northeastern University	
Dr. Amy Peikoff	Bit Chute Limited	
Ms. Riana Pfefferkorn	Stanford University	
Dr. Amreesh Phokeer	Internet Society	
Prof. Michalis Polychronakis	Stony Brook University	
Dr. Niels Provos	Independent researcher	
Prof. Sazzadur Rahaman	University of Arizona	
Prof. Amir Rahmati	Stony Brook University	
Prof. Aanjhan Ranganathan	Northeastern University	
Prof. Franziska Roesner	University of Washington	
Prof. Ronald L. Rivest	MIT	Turing Award
Dr. Sarah Scheffler	Princeton University	
Prof. Barbara van Schewick	Stanford University	
Prof. Bruce Schneier	Harvard Kennedy School	
Prof. Adam Shostack	University of Washington	
Prof. Eugene H. Spafford	University of Purdue	
Dr. Christian Straka	Yale University	
Mr. Nick Sullivan	Independent	
Dr. Gilian Tenbergen	Prostasia Foundation	
Dr. Alin Tomescu	Aptos Lab	
Dr. Santiago Torres-Arias	Purdue University	
Prof. Blase Ur	University of Chicago	
Prof. Ersin Uzun	Rochester Institute of Technology	
Prof. Daniel Votipka	Tufts University	
Prof. David Wagner	UC Berkeley	
Prof. Daniel J. Weitzner	MIT	
Dr. Lian Wang	Princeton University	
Prof. Christo Wilson	Northeastern University	Sloan Fellow
Prof. Matthew Wright	Rochester Institute of Technology	