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, Fundaçao 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	Canada Research Chair
Dr. Simón Oya	University of Waterloo	
Prof. Nicolas Papernot	University of Toronto and Vector Institute	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	Fellow IACR
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	

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	Inria
Dr. Veronique Cortier	CNRS
Dr. Jannik Dreier	Université de Lorraine
Prof. Antonio Faonio	EURECOM
Dr. Caroline Fontaine	CNRS
Dr. Aurélien Francillon	EURECOM
Dr. Aymeric Fromherz	Inria
Dr. Pierrick Gaudry	CNRS
Prof. Elham Kashefi	CNRS and University of Edimburgh
Dr. Jonathan Keller	Institut Mines Telecom
Dr. Nadim Kobeissi	Symbolic Software
Dr. Steve Kremer	Inria
Dr. Gaëtan Leurent	Inria
Dr. Pierre Laperdrix	CNRS
Dr. Victor Lomné	NinjaLab
Dr. P. G. Macioti	Medicines du Monde
Dr. Clémentine Maurice	CNRS
Hon. Dr. Traian Muntean	Aix-Marseille University
Prof. Melek Önen	EURECOM
Dr. Maria Naya Plasencia	Inria
Dir. Research Catuscia Palamidessi	Inria
Dr. Léo Perrin	Inria
Dr. Peter Roenne	CNRS
Dr. Yann Rote	Université Paris-Saclay
Dr. Emmanuel Thomé	Inria
Dr. Anna Weine	Mozilla

Germany

Dr. Ali Abassi	CISPA Helmholtz Center for Information Security
Prof. Patricia Arias Cabarcos	Paderborn University
Prof. Dr. Alexander Auch	Baden-Wuerttemberg Cooperative State University
Dr. Gilles Barthe	Max Planck Institute for Security and Privacy
Dr. Steffen Becker	Ruhr University Bochum & Max Planck Institute for Security and Privacy
Prof. Dr. Bettina Berendt	TU Berlin and KU Leuven
Dr. Sebastian Berndt	University of Lübeck
Dr. Asia Biega	Max Planck Institute for Security and Privacy
Dr. Christopher Blöcker	Julius-Maximilians-Universität Würzburg
Dr. Marcel Böhme	Max Planck Institute for Security and Privacy
Dr. Harald Böhme	ANSYS Germany
Prof. Dr. Kevin Borgolte	Ruhr University Bochum
Dr. Sven Bugiel	CISPA Helmholtz Center for Information Security
Dr. Rebekka Burkholz	CISPA Helmholtz Center for Information Security
Dr.-Ing. Jiska Classen	Hasso Plattner Institute
Prof. Dr. Cas Cremers	CISPA Helmholtz Center for Information Security
Prof. Dr.-Ing. Alexandra Dmitrienko	Julius-Maximilians Universität Würzburg
Prof. Thomas Eisenbarth	University of Lübeck
Prof. Sebastian Faust	Technical University of Darmstadt
Dr.-Ing. Daniel Demmler	Personal Capacity
Dr. Christian Gollwitzer	Physikalisch-Technische Bundesanstalt
Dr. Dominik Helm	Technische Universität Darmstadt
Prof. Dr. Jeanette Hofmann	Berlin Social Science Center
Prof. Thorsten Holz	CISPA Helmholtz Center for Information Security
Prof. Matthias Hollick	Technical University of Darmstadt
Dr. Julian Hoth	Hamburg University of Technology
Prof. Tibor Jager	University of Wuppertal
Prof. Dr. Stefan Katzenbeisser	University of Passau
Dr. Dietmar Kammerer	Weizenbaum Institute for the Networked Society
Dr. Elif Bilge Kavun	University of Passau
Dr. Franziskus Kiefer	Cryspen

Prof. Dr. phil Thomas Knaus	PH Ludwigsburg | FTzM Frankfurt/Main
Dr. Katharina Krombholz	CISPA Helmholtz Center for Information Security
Prof. Anja Lehmann	Hasso-Plattner-Institute, University of Potsdam
Dr. Ferdinand Lehmann	Justus Liebig Universität Gießen
Prof. Dr. Daniel Loebenberger	Fraunhofer AISEC / OTH Amberg-Weiden
Dr. Alexander Loew	DWH
Dr. Wouter Lueks	CISPA Helmholtz Center for Information Security
Dr. Genia Lücking	Technical University of Munich
Dr. Thomas Mager	Personal capacity
Dr. Christian Mainka	Ruhr University Bochum
Dr. Jens Meier	Deutsches Institut für Kautschuktechnologie e.V.
Prof. Dr. Esfandiar Mohammadi	University of Lübeck
Dr. Veelasha Moonsamy	Ruhr University Bochum
Prof. Dr. Andreas Peter	University of Oldenburg
Dr. Giancarlo Pellegrino	CISPA Helmholtz Center for Information Security
Dr. Henrich C. Pöhls	University of Passau
Prof. Joachim Posegga	University of Passau
Prof. Dr. Kai Rannenberg	Goethe University Frankfurt
Dr. Elissa Redmiles	Max Planck Institute for Software Systems
Dipl. Inf. Rainer Rehak	Weizenbaum Institute for the Networked Society
Prof. Konrad Rieck	Technische Universität Berlin
Prof. Stefanie Roos	University of Kaiserslautern-Landau
Prof. Paul Rösler	FAU Erlangen-Nürnberg
Prof. Dr. Christian Rossow	CISPA Helmholtz Center for Information Security
Prof. Dr. Christoph Skornia	University of Applied Sciences Regensburg
Dr. Jens Schade	TU Dresden
Prof. Dr. Sebastian Schinzel	Münster University of Applied Sciences
Prof. Thomas Schneider	Technische Universität Darmstadt
Prof. Dr. Marc C. Steinbach	Leibniz Universität Hannover
Prof. Dr. Dominique Schröder	Friedrich-Alexander Universität Erlangen-Nürnberg
Dr. Peter Schwabe	Max Planck Institute for Security and Privacy
Dipl. Ir. Peter Schoo	Personal Capacity Fellow ACM
Prof. Dr. Ingo Scholtes	Julius-Maximilians-Universität Würzburg
Prof. Juraj Somorovsky	Paderborn University
Prof. Dr. Christoph Sorge	Saarland University
Dr. Ben Stock	CISPA Helmholtz Center for Information Security
Prof. Thorsten Strufe	KASTEL/Karlsruhe & Centre for Tactile Internet with Human-in-the-Loop, Dresden
Prof. Florian Tschorsch	TU Berlin and HU Berlin
Dr. Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security
Dr. Anjo Vahldiek-Oberwagner	Intel Labs
Dr. Vera Wilde	Freelance
Prof. Christian Wressnegger	Karlsruhe Institute of Technology
Prof. Dr. Yuval Yarom	Ruhr University Bochum
Dr. Xiao Zhang	CISPA Helmholtz Center for Information Security
Dr. Yixin Zou	Max Planck Institute for Security and Privacy

Greece

Prof. Vasiliki Diamantopoulou	University of the Aegean
Prof. Christos Kalloniatis	University of the Aegean
Prof. Georgios Kambourakis	University of the Aegean
Dr. Platon Kotzias	Norton Research Group
Prof. Costas Lambrinoudakis	University of Piraeus
Prof. Emmanouil Magkos	Ionian University
Prof. Stefanos Gritzalis	University of Piraeus and Hellenic Authority for Communication Security and Privacy
Prof. Panagiotis Rizomiliotis	Harokopio University of Athens

Hungary

Dr. Gergely Biczók	Budapest Univ. of Technology and Economics
Dr. Balazs Pejo	Budapest Univ. of Technology and Economics

Ireland

Dr. Stephen Farrell	Trinity College Dublin
Dr. Aikaterini Kanta	University College Dublin
Prof. Douglas Leith	Trinity College Dublin
Dr. TJ McIntyre	University College Dublin Sutherland School of Law & Digital Rights Ireland
Dr. Kris Shrishak	Irish Council for Civil Liberties

India

Dr. Chaya Ganesh	Indian Institute of Science

Israel

Prof. Orr Dunlekman	University of Haifa
Dr. Yossi Oren	Ben-Gurion University
Dr. Eyal Ronen	Tel Aviv University
Dr. Mahmood Sharif	Tel Aviv University

Italy

Prof. Stefano Calzavara	Università Ca' Foscari Venezia
Prof. Mauro Conti	University of Padua
Prof. Bruno Crispo	University of Trento
Prof. Paolo Falcarin	University of Venice
Prof. Fabio Massaci	University of Trento/Vrije Universiteit Amsterdam
Dr. Daniela Morpurgo	Politecnico di Torino
Prof. Giuseppe Persiano	Università di Salerno
Dr. Dario Stabili	University of Bologna
Prof. Daniele Venturi	Sapienza University of Rome
Prof. Stefano Zanero	Politecnico di Milano

Japan

Prof. Em. Toshimaru Ogura	Toyama University
Prof. Takao Murakami	The Institute of Statistical Mathematics (ISM)
Prof. Kazue Sako	Waseda University

Liechtenstein

Prof. Giovanni Apruzzese	University of Liechtenstein

Luxembourg

Dr. Orham Ermis	Luxembourg Institute of Science and Technology
Dr. Aditya Damodaran	University of Luxembourg
Prof. Dr. Gabriele Lenzini	University of Luxembourg
Prof. Peter Y A Ryan	University of Luxembourg

Mexico

Prof. Alejandro Pisanty	Universidad Nacional Autónoma de México

The Netherlands

Dr. Gunes Acar	Radboud University Nijmegen
Prof. Dr. Lejla Batina	Radboud University Nijmegen
Prof. Dr. LLM Frederik Z. Borgesius	iHub, Radboud University
Prof. Dr. ir. Herbert Bos	Vrije Universiteit Amsterdam
Dr. Corinne Cath	Delft University of Technology
Dr. Andrea Continella	University of Twente
Prof. Ronald Cramer	CWI & Leiden University
Dr. Lorenzo Dalla Corte	Tilburg University
Prof. Joan Daemen	Radboud University Nijmegen

Prof. Dr. Arie van Deursen	Delft University of Technology
Dr. Ir. Roel Dobbe	Delft University of Technology
Dr. Zekeriya Erkin	Delft University of Technology
Prof. Cristiano Giuffrida	Vrije Universiteit Amsterdam
Dr. Seda Gürses	Delft University of Technology
Dr. Florian Hahn	University of Twente
Prof. Jaap-Henk Hoepman	Radboud University Nijmegen
Prof. Andreas Hülsing	Eindhoven University of Technology
Dr. Georgy Ishmaev	Delft University of Technology
Prof. Bart Jacobs	Radboud University Nijmegen
Dr. Konrad Kollnig	Maastricht University
Dr. Matthijs Koot	University of Amsterdam & Secura BV
Dr. Ralph Koning	University of Amsterdam
Prof. Eleni Kosta	Tilburg University
Prof. Dr. Tanja Lange	Eindhoven University of Technology
Dr. Luca Mariot	University of Twente
Dr. Giovane Moura	Delft University of Technology
Dr. Laurens Naudts	University of Amsterdam
Dr. Fatih Turkmen	University of Groningen
Prof. Georgios Smaragdakis	Delft University of Technology
Dr. Kitty Smeekes	Personal capacity
Prof. Ot van Daalen	University of Amsterdam
Prof. Michel van Eeten	Delft University of Technology
Dr. Jeroen van der Ham	University of Twente
Prof. dr. Ir. Roland van Rijswijk-Deij	University of Twente
Dr. Heloise Vieira	Eindhoven University of Technology
Prof. Ben Wagner	Delft University of Technology

New Zealand

Prof. Brian E. Carpenter	University of Auckland
Prof. Steven Galbraith	University of Auckland

Norway

Prof. Anamaria Costache	Norwegian University of Science and Technology
Prof. Danilo Gligoroski	Norwegian University of Science and Technology
Dr. Erik Hjelmås	Norwegian University of Science and Technology
Prof. Helger Lipmaa	Simula UiB
Prof. Sokratis Katsikas	Norwegian University of Science and Technology
Prof. Paweł Morawiecki	Polish Academy of Sciences
Dr. Vinit Ravishankar	University of Oslo
Prof. David Palma	Norwegian University of Science and Technology
Prof. Tjerand Silde	Norwegian University of Science and Technology
Prof. Mohsen Toorani	University of South-Eastern Norway
Prof. Øyvind Ytrehus	Simula UiB and University of Bergen
Prof. Thomas Zinner	Norwegian University of Science and Technology

Poland

Prof. Stefan Dziembowski	University of Warsaw
Prof. Wojciech Jamroga	Institute of Computer Science, Polish Academy of Sciences
Dr. Dariusz Kalociński	Institute of Computer Science, Polish Academy of Sciences
Dr. Anna Ratecka	Jagiellonian University in Krakow

Portugal

Ms. Sofia Celi	Brave
Prof. Manuel Eduardo Correia	University of Porto
Prof. Manuel Barbosa	University of Porto and INESC TEC
Prof. Hugo Pacheco	University of Porto
Prof. Bernardo Portela	University of Porto
Prof. Henrique Santos	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	Universidad Politécnica de Madrid	
Prof. Pino Caballero-Gil	University of La Laguna	
Dr. Ignacio Cascudo	IMDEA Software Institute	
Prof. Josep Domingo-Ferrer	Universitat Rovira i Virgili	Fellow IEEE
Dr. Dario Fiore	IMDEA Software Institute	
Prof. Jose Maria de Fuentes	Universidad Carlos III de Madrid	
Dr. Gemma Galdon Clavell	Eticas Tech	
Prof. Maribel González Vasco	Universidad Carlos III de Madrid	
Prof. Lorena González Manzano	Universidad Carlos III de Madrid	
Dr. Marco Guarnieri	IMDEA Software Institute	
Prof. Simona Levi	Xnet and University of Barcelona	
Dr. Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona	
Prof. Llorenç Huguet	Balearic Island University	
Dr. Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona	
Prof. Fernando Pérez-González	University of Vigo	Fellow IEEE
Dr. Cristina Perez-Sola	Universitat Autònoma de Barcelona	
Dr. Helena Rifà-Pous	Universitat Oberta de Catalunya	
Dr. Guillermo Suarez-Tangil	IMDEA Networks Institute	
Prof. Jose Such	Universitat Politecnica de Valencia	
Dr. Carla Ràfols	Universitat Pompeu Fabra	
Prof. Josep Rifà	Universitat Autònoma de Barcelona	
Prof. Juan Tapiador	Universidad Carlos III de Madrid	
Dr. Narseo Vallina-Rodriguez	IMDEA Networks Institute	

Sweden

Prof. Simone Fischer-Hübner	Karlstad University & Chalmers University of Technology	
Prof. Dr.-Ing.Meiko Jensen	Karlstad University	
Dr. Victor Morel	Chalmers University	
Prof. Panos Papadimitratos	KTH Royal Institute of Technology	Fellow IEEE
Dr. Pablo Picazo-Sanchez	Halmstad University	
Dr. Tobias Pulls	Karlstad University	
Dr. Iraklis Symeonidis	RISE	
Prof. Vicenç Torra	Umeå University	Fellow IEEE

Switzerland

Dr. Anthony Boulmier	OptumSoft Inc.	
Dr. Jonathan Bootle	Personal capacity	
Prof. Srdjan Capkun	ETH Zurich	Fellow IEEE
Prof. Bryan Ford	EPFL	
Dr. Jens Groth	DFINITY	
Dr. Julia Hesse	IBM Zurich	
Prof. Jean-Pierre Hubaux	EPFL	Fellow ACM
Dr. Kari Kostianen	ETH Zurich	
Dr. Anil Kurmus	Personal Capacity	
Dr. Siniša Matetić	ETH Zurich	
Prof. Marc Langheinrich	Università della Svizzera italiana	

Dr. Onicio Batista Leal Neto	ETH Zurich	
Prof. Rebekah Overdorf	University of Lausanne	
Prof. Kenneth Paterson	ETH Zurich	Fellow IACR
Prof. Mathias Payer	EPFL	
Dr Ivan Puddu	ETH Zurich	
Dr. Apostolos Pyrgelis	EPFL	
Prof. Kaveh Razavi	ETH Zurich	
Dr. Raphael M. Reischuk	National Test Institute for Cybersecurity NTC	
Dr. Benjamin Rothenberger	Zühlke Engineering AG	
Dr. Alessandro Sorniotti	Personal capacity	
Prof. Shweta Shinde	ETH Zurich	
Prof. Dr. Florian Tramèr	ETH Zurich	
Prof. Carmela Troncoso	EPFL	

Taiwan

Dr. Lorenz Panny	Academia Sinisa

Turkey

Prof. Mehmet Tahir Sandikkaya	Istanbul Technical University
Prof. Cihangir Tezcan	Middle East Technical University

United Arab Emirates

Prof. Michail Maniatakos	New York University Abu Dhabi
Dr. Victor Mateu	Technology and Innovation Institute
Prof. Chirstina Pöpper	New York University Abu Dhabi

United Kingdom

Dr. Ruba Abu-Salma	King’s College London
Prof. Martin Albrecht	King’s College London
Dr. Panagiotis Andriotis	University of Birmingham
Prof. Ross Anderson	Universities of Cambridge and Edinburgh
Dr. Andrea Basso	University of Bristol
Dr. Pascal Berrang	University of Birmingham
Prof. Alastair Beresford	University of Cambridge
Prof. Reuben Binns	University of Oxford
Prof. Ioana Boureanu	University of Surrey
Dr. Jaya Klara Brekke	Nym Technologies
Prof. Lorenzo Cavallaro	University College London
Dr. Michele Ciampi	University of Edinburgh
Dr. George Chalhoub	University of Oxford
Prof. Liqun Chen	University of Surrey
Dr. Richard Clayton	University of Cambridge
Dr. Kovila Coopamootoo	King’s College London
Prof. Angela Daly	University of Dundee
Dr. Partha Das Chowdhury	University of Bristol
Dr. Santanu Dash	Royal Holloway, University of London
Dr. Benjamin Dowling	University of Sheffield
Dr. François Dupressoir	University of Bristol
Dr. Tariq Elahi	University of Edinburgh
Dr. Pooya Farshim	Durham University
Prof. Hamed Haddadi	Imperial College London
Prof. Julio Hernandez-Castro	University of Kent
Dr. Alice Hutchings	University of Cambridge
Dr. Martin Husovec	London School of Economics and Political Science
Dr. Dennis Jackson	Mozilla
Dr. Rikke Jensen	Royal Holloway, University of London
Dr. Vitor Jesus	Aston University
Prof. Adam Joinson	University of Bath
Dr. Philipp Jovanovic	University College London

Prof. Vasilis Katos	Bournemouth University	
Prof. Markulf Kohlweiss	University of Efinburgh	
Dr. Kopo Marvin Ramokapane	University of Bristol	
Prof. Aggelos Kiayias	University of Edinburgh	
Dr. Bernardo Magri	University of Manchester	
Prof. Corinne May-Chahal	University of Lancaster	
Prof. Keith Martin	Royal Holloway, University of London	
Dr. Maryam Mehrnezhad	Royal Holloway, University of London	
Prof. Sarah Meiklejohn	University College London	
Prof. Steven Murdoch	University College London	
Prof. Douwe Korff	London Metropolitan University	
Dr. Daniel Page	University of Bristol	
Dr. Claudia Peersman	University of Bristol	
Prof. Andy Phippen	Bournemouth Universiy	
Dr. Fabio Pierazzi	King’s College London	
Prof. Awais Rachid	University of Bristol	
Dr. Luc Rocher	University of Oxford	
Dr. Kaspar Rosager Ludvigsen	University of Edinburgh	
Dr. Christos Sagredos	King’s College London	
Dr. Siamak Shahandashti	University of York	
Prof. Tom Stoneham	University of York	
Dr. Jose Tomas Llanos	University College London	
Dr. Michael Veale	University College London	
Dr. Niovi Vavoula	Queen Mary University of London	
Dr. Christian Weinert	Royal Holloway, University of London	
Prof. Alan Woodward	University of Surrey	
Dr. Joss Wright	University of Oxford	

United States of America

Prof. Giuseppe Ateniese	George Mason University	
Prof. Adam J. Aviv	George Washington University	
Prof. Steven Bellovin	Columbia University	
Prof. Matt Blaze	Georgetown University	McDevitt Chair of CS and Law
Prof. Kevin Butler	University of Florida	
Mr. Jon Callas	Personal capacity	
Prof. Álvaro Cárdenas	University of California, Santa Cruz	
Prof. Chandrasekaran	University Illinois Urbana-Champaign	
Prof. David Choffnes	Northeastern University	
Prof. Nicolas Christin	Carnegie Mellon University	
Mr. Roger Dingledine	The Tor Project	
Prof. Tudor Dumitras	University of Maryland	
Prof. Zakir Durumeric	Stanford University	
Prof. Joan Feigenbaum	Yale University	ACM Fellow
Prof. Michael J. Fischer	Yale University	ACM Fellow
Dr. Kelsey Fulton	Colorado School of Mines	
Dr. Simson L. Garfinkel	Digital Corpora Project	Fellow AAAS, ACM, IEEE
Prof. Christina Garman	Purdue University	
Prof. Matthew D. Green	Johns Hopkins University	
Prof. Daniel Genkin	Georgia Tech	
Prof. Paul Grubbs	University of Michigan	
Dr. Joseph Lorenzo Hall	Internet Society	
Dr. Britta Hale	Independent researcher	
Prof. Emeritus Martin Hellman	Stanford University	Turing Award
Prof. Nadia Heninger	University of California, San Diego	
Prof. Amir Herzberg	University of Connecticut	
Prof. Peter Honeyman	University of Michigan	
Prof. Nicholas Hopper	University of Minnesota	
Prof. Gabriel Kaptchuk	Boston University	
Prof. Vasileios Kemerlis	Brown University	
Dr. Jennifer King	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	