This letter can be found at: https://csa-scientist-open-letter.org/Sep2025

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 Sept 9 2025
Signatories: 502
Countries: 34

For press inquiries please contact:

Austria	René Mayrhofer - rm@ins.jku.at
Belgium	Bart Preneel - bart.preneel@esat.kuleuven.be
Czech Republic	Vashek Matyas - matyas@fi.muni.cz
Denmark	Diego Aranha - dfaranha@cs.au.dk
Finland	Kimmo Halunen - Kimmo.Halunen@oulu.fi
France	Aurelien Francillon - aurelien.francillon@eurecom.fr
Germany	Thorsten Holz - thorsten.holz@mpi-sp.org
Germany	Cas Cremers - cremers@cispa.de
Ireland	Stephen Farrell - stephen.farrell@cs.tcd.ie
Israel	Eyal Ronen - eyal.ronen@cs.tau.ac.il
Italy	Stefano Zanero - stefano.zanero@polimi.it
Norway	Tjerand Silde - tjerand.silde@ntnu.no
Poland	Stefan Dziembowski stefan.dziembowski@crypto.edu.pl
Spain	Carmela Troncoso - carmela.troncoso@epfl.ch
Switzerland	Carmela Troncoso - carmela.troncoso@epfl.ch
The Netherlands	Jaap-Henk Hoepman - jhh@cs.ru.nl
UK	Michael Veale - m.veale@ucl.ac.uk

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/ResearchersCSAOct25** (PhD or demonstrated research track record required)

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

9th September 2025 - Joint statement of scientists and researchers on the EU Presidency's new proposal for the Child Sexual Abuse Regulation

We are writing in response to the new proposal by the Presidency dated 24 July 2025.

We share your concerns about the abuse of children in hideous crimes, resulting in serious harms to the victims and their families. In view of this, we are pleased to note the improvements in the new draft of the regulation proposal including the incorporation of some of the recommendations in our letters of July 2023, May 2024, and September 2024. We particularly appreciate the addition of provisions to ease the voluntary reporting of illegal activity, and the requirement to accelerate the treatment of these reports. These are essential to guarantee swift and effective help for victims of abuse.

However, we read in dismay how none of the changes address our major concerns: it is simply not feasible to perform detection of known and new CSAM for hundreds of millions of users with an acceptable level of accuracy, independently of the specific filter. Moreover, on-device detection, regardless of its technical implementation, inherently undermines the protections that end-to-end encryption is designed to guarantee. Even worse, the changes in the proposal increase the reliance on technical means to support its goals, exacerbating the security and privacy risks for citizens without any guarantee of improved protection for children. We elaborate on these issues below.

The new proposal, similar to its predecessors, will create unprecedented capabilities for surveillance, control, and censorship and has an inherent risk for function creep and abuse by less democratic regimes. Achieving current security and privacy of digital communications and systems has taken decades of concerted effort by researchers, industry, and policy makers. There is no doubt that this proposal completely undermines the security and privacy protections that are essential to protect the digital society.

We also regret that policy makers have failed to create an open dialogue with experts on this topic in the last two years. In spite of the serious doubts on the effectiveness of detection technologies, there has been no public discussion, analysis, and assessment of these technologies that could justify the approach taken in the proposed regulation. This lack of transparency hinders an open and informed discussion that can identify suitable technologies to address children's abuse, and endangers the digital safety of our society in Europe and beyond.

1. The changes to reduce the scope of targeted material will not increase effectiveness

A major change being considered by the Council is that the proposed detection of CSAM (Child Sex and Abuse Material) only applies to **images** (visual information) and **URLs**. This is in contrast to previous versions of the proposal in which detection would be applied to any material sent between users (including text and audio). This change aims to reduce the scope of the proposal by limiting it to specific file formats, in order to increase the proposal's proportionality with respect to the intended goals, and avoid the issues associated with detection of illegal behaviour such as grooming in text.

While a reduction in scope is certainly welcome, it does not eliminate any of the serious concerns raised in our previous letters. There is no scientific basis to argue that detection technology would work any better on images than on text (see our first letter for more details). Experts have repeatedly shown that detection methods for known CSAM are easy to evade: changing a few bits in an image is sufficient to ensure that an image will not trigger state-of-the-art detectors. And while it may seem that keeping the detection algorithm a secret could prevent evasion, the latest work on this topic shows that these types of attacks can be effective even without knowing the algorithm used by the detection mechanism. Thus, those wanting to distribute CSAM will soon adopt these methods, completely bypassing the detection mechanism. **Existing research confirms that state-of-the-art detectors would yield unacceptably high false positive and false negative rates, making them unsuitable for large-scale detection campaigns at the scale of hundreds of millions of users as required by the proposed regulation**.

The current proposal further reintroduces the possibility of using machine learning and artificial intelligence to also detect unknown CSAM images. We reiterate that to the best of our knowledge there is no machine-learning algorithm that can perform such detection without committing a large number of errors (e.g., distinguishing between CSAM material and sexting teenagers is hard even for humans), and that all known algorithms are fundamentally susceptible to evasion. Besides all the existing attacks, once detection is mandatory we expect to see many more attacks developed by those motivated to share illicit material. **Given that AI-based technologies have an enormous attack surface, and that it is impossible to fully eliminate this surface, we expect these technologies to be highly ineffective in the case of CSAM detection.**

Beyond visual information, the new proposal additionally requests to check URLs for illegitimate content. Evasion is even easier for URLs: Redirection of URLs is trivial, via commercial services or locally, and can be done seamlessly even by unskilled users. The vast number of ways in which URLs can easily be changed, make the detection of malicious URLs a notable open problem, even though it is central to web security in general. In fact, similar challenges are faced in the context of intrusion detection, malware identification, or ad-blocking. Despite being widely researched by industry and academia, this problem is notoriously unsolvable, and detectors tend to *not* use URLs as an input to avoid manipulations that reduce the effectiveness of the detector. **There is no reason to believe that when it comes to URLs hosting CSAM the result would be any different than in other fields where malicious URLs cannot be identified**.

Intuitively, on-device CSAM scanning might seem similar to malware checks by antivirus software, but the two are fundamentally different. Malware detection works well when it can target clear, well-defined threats, whereas CSAM detection is inherently contextual and cannot be technically defined with certainty—for example, teenagers' consensual texting, medical photos, or family vacation images. As a result, CSAM detectors fundamentally cannot match the reliability of malware scanners. Moreover, if potential malware is found on a consumer device, the user is asked to make a decision. That is, malware scanning is voluntary, transparent, and not tied to law enforcement backdoors. Mandating on-device CSAM scanning, and providing law enforcement with access to any image matched by the algorithm, is incompatible with all these safeguards.

In conclusion, the changes in the proposal do not address the main shortcoming: existing detection technology is far from achieving the high accuracy level required in the context of CSA protection; and all security and privacy research on the field indicate that the issues that make them unreliable are inherent and will not be eliminated in the future. **Thus, there is no evidence that the changes in scope of detection makes any effective difference with respect to the previous proposal**.

2 On device detection inherently removes encryption protection

The proposal demands that the CSAM detection technology shall not lead to a *"weakening of the protection provided by encryption"*. We absolutely agree with this view: End-to-End-Encryption (E2EE) is essential to enable EU citizens to communicate securely and privately online, in particular when considering that core parts of our communication infrastructure are controlled by US Big Tech and many nation states have expanded their interception capabilities, both on-device and on-path. Encryption protects not only the civil society, but **EU politicians, decision makers, law enforcement, and defence forces also critically rely on E2E-encryption** to ensure secure communications against internal and external threats.

However, it is impossible to perform any detection of material and send subsequent reports without affecting encryption. The core design principles of secure end-to-end encryption protection include (i) ensuring that only the intended two endpoints can access the data, and (ii) avoiding a single point of failure. Enforcing a detection mechanism to scan private data before it gets encrypted – with the possibility to transmit it to law enforcement upon inspection – inherently violates both principles: **it undermines the functionality of E2EE by accessing the private data through the detecting mechanism and introduces a single point of failure into all our secure E2EE mechanisms through these enforced detections**.

In fact, the detection mechanism substantially increases the attack surface and becomes a high-value target for threat actors themself. The mechanism cannot be technically limited to the detection of CSAM, or the targeting of visual information and URLs. It is trivial to reconfigure it to identify other types of data, and target further types of information related to other crimes or to financial or political interests (e.g., memes about political parties). Moreover, the current reduction in scope only seems to be a temporary appeasement, and the changelog of the proposed regulation [related to grooming, p.2, p.4] suggests that the scope will in the future again be extended to audio and text. In other words, **the new proposal does not address our concerns regarding the potential for function creep of on-device detection.**

The new proposal also reinforces previous changes to reduce the scope of detection to so-called "high-risk" parts or components of services. **Yet, the definition of high-risk would cover some services in their entirety.** A paramount example is E2E encrypted messaging, such as Signal or WhatsApp, used by regular citizens but also politicians, journalists, human-right workers, EU civil servants, and law enforcement officers. Should the proposal be approved, the protection provided by these apps would evaporate – which has led Signal to announce that they would stop their service in the EU should on-device detection become mandatory, as any realization would inherently break with the promise of E2EE and put users at risk.

Finally, detection would require handling data outside of the scope of the E2EE. This implies that private communications content suspected of being CSAM (but not guaranteed to be so, as per our first point) will leave the device of the user, and potentially be accessed by national authorities. This is parallel to the case of Podchasov v. Russia, for which the European Court of Human Rights reiterates that **the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (the right to privacy)**.

In conclusion, **the new proposal's implications unequivocally violate basic E2EE principles and *will* weaken the protection provided by encryption**. Furthermore, this weakening threatens our fundamental right to privacy and can have severe consequences on our democratic processes and national security by preventing digital confidential communications.

3. Mandating the use of all possible technical mitigations does not increase security

Another critical change in the new proposal is to make it mandatory for service providers to take "***all** reasonable measures to mitigate the risk of their service being used for abuse*", and includes new provisions to foster and regulate the use of "*age verification and age assessment measures*".

We first highlight that in security, taking additional measures does not always result in increased protection. Introducing new mitigations might reduce the protection of the system to the protection offered by the weakest mitigation, while increasing the complexity – and therefore also risks – for the overall system. In the case of this proposal, **given the inadequacy of detection technologies as explained in the previous point, the addition of other mitigations can bring little extra protection to users and victims.**

Further, we do not believe that mandating age verification techniques to control the access to content on the Internet will bring the desired benefits. First, age verification controls can be evaded with ease. We have witnessed this in the UK, where the implementation of the Online Safety Act resulted in users turning to services that do not implement the controls -- which will always happen as long as there are services in the world that do not implement them. The UK also observed a surge of VPN connections to bypass the verification by accessing servers from other locations. Moreover, this leads to new risks. The mandatory character of age verification can become a reason to ban the use of privacy technologies such as VPNs that can help to circumvent it. This would threaten freedom of speech and freedom of information by preventing users from privately browsing the Internet and undermines the tools needed by whistleblowers, journalists and human right activists. It would also have devastating effects on the security of the web as VPNs are a security backbone for industry to enable the use of internal and external remote services.

Second, even if age verification is implemented with verifiable and certified attributes, as in the new age verification app of the EU, it still erodes fundamental principles of online anonymity and open access to information. Initially, such technology might only be demanded for proving that one is older than 18 years old, but once in place, the same technology can be used to demand the disclosure of other and more identifying information such as gender, nationality, or medical conditions. Before rolling them out, evidence is needed on the benefits that introducing such technology would bring, and evidence that the harms it introduces (e.g., potential for tracking or censorship) can be mitigated.

Furthermore, we are also concerned that the sudden pressure to implement such solutions might result in rushed decisions. Early prototypes by some Big Tech providers have not been studied in depth and lack open peer review; their use would not only entail a risk in terms of performance but will also create a dependency on Big Tech for Europe in a critical infrastructure aimed to protect children.

We conclude that increasing the number of technologies used to address the Child Sexual Abuse problem, and making them mandatory not only does not improve on the previous proposal but **increases its problems and broadens the potential negative impact of this proposed regulation on the security of the Internet and the freedom and privacy of its users**.

4. Secure paths forward for child protection

Two years after our first letter, we want to reiterate that given the limitations of technology, the current techno-solutionist proposal with main focus on removing abusive material from the internet at the cost of communication security, has little potential for impact on abuse perpetrated against children.

We remind that CSAM content is the output of child sexual abuse. Eradicating CSAM therefore, relies on eradicating abuse, not only on preventing the digital dissemination of abuse material. Instead of continuing the push to technologies with dubious effectiveness such as CSAM detection algorithms and age verification that significantly weaken security and privacy, we want to call again attention to the measures recommended by organisations such as the UN. These include education (on consent, norms and values, on digital literacy and online safety, and comprehensive sex education); trauma-sensitive reporting hotlines; and keyword-search based interventions.

The steps towards better reporting and faster removal are great advances, but we reiterate our recommendation to substantially increase investment and effort in supporting proven approaches towards eradicating abuse. By eliminating abuse, these measures will also eradicate abusive material without introducing any risk to secure digital interactions which are essential for the safety of the children the proposed regulation aims to protect.

Signatories

Australia

Prof. Qiang Tang	The University of Sydney
A/Prof. Vanessa Teague	Thinking Cybersecurity Pty Ltd, Australian National University

Austria

Prof. Dr. Elena Andreeva	TU Wien
Prof. Maria Eichlseder	Graz University of Technology
Prof. Daniel Gruss	Graz University of Technology

Dr. Walter Hötzendorfer	Research Institute – Digital Human Rights Center
Prof. Martina Lindorfer	TU Wien
Univ.-Prof. Dr. Matteo Maffei	TU Wien
Univ.-Prof. Dr. Stefan Mangard	Graz University of Technology
Prof. René Mayrhofer	Johannes Kepler University Linz
Dr. Stefan More	Graz University of Technology
Prof. Krzysztof Pietrzak	Institute of Science and Technology Austria
Univ.-Prof. Dr. Christian Rechberger	Graz University of Technology
Prof. Sujoy Sinha Roy	Graz University of Technology
Dr. Diogo Sasdelli	Universität für Weiterbildung Krems
Prof. Dr. Peter Schartner	Klagenfurt University
Univ.-Prof. Dr. Dominique Schröder	TU Wien
Prof. Mag. Dr. Wieland Schwinger	Johannes Kepler University Linz
Marek Sefranek	TU Wien
Ing. Dr.iur. Christof Tschohl	Research Institute – Digital Human Rights Center
Prof. Edgar Weippl	University of Vienna

Belgium

Dr. Aysajan Abidin	KU Leuven
Dr. Emad Heydari Beni	KU Leuven
Prof. Tijl De Bie	Ghent University
Dr. Rosamunde Van Brakel	Vrije Universiteit Brussel
Dr. Gaetan Cassiers	UCLouvain

Prof. Quentin De Coninck	UMONS
Prof. Claudia Diaz	KU Leuven
Prof. Laura Drechsler	KU Leuven/State Archives of Belgium/Open Universiteit
Prof. Jean-Michel Dricot	Université Libre de Bruxelles
Prof. Dr. Gloria Gonzalez Fuster	Vrije Universiteit Brussel
Dr. Mariana Gama	KU Leuven
Dr. Benedikt Gierlichs	KU Leuven
Dr. Milos Grujic	KU Leuven
Dr. Iness Ben Guirat	Université Libre de Bruxelles
Prof. Paul De Hert	Vrije Universiteit Brussel
Dr. Francois Koeune	UCLouvain
Dr. Diane Leblanc-Albarel	KU Leuven
Dr. Barry van Leeuwen	KU Leuven
Dr. Ingrida Milkaite	Vrije Universiteit Brussel
Dr. Thorben Moos	UCLouvain
Prof. Yves Moreau	KU Leuven
Prof. Jan Tobias Muehlberg	Universite Libre de Bruxelles
Dr. Svetla Nikova	KU Leuven
Dr. Charles-Henry Bertrand Van Ouytsel	UCLouvain
Dr. Roel Peeters	KU Leuven
Prof. Olivier Pereira	UCLouvain
Prof. Thomas Peters	UCLouvain & FNRS
Prof. Bart Preneel	KU Leuven
Dr. Frederik Questier	Vrije Universiteit Brussel

Prof. Jean-Jacques Quisquater	UCLouvain
Mr. Sam van Rijn	PXL University of Applied Sciences and Arts
Dr. Vera Rimmer	KU Leuven
Prof. Etienne Riviere	UCLouvain
Prof. Florentin Rochet	UNamur
Prof. Sofie Royer	KU Leuven and ULiège
Dr. Enrique Argones Rúa	KU Leuven
Prof. Wim Schoutens	KU Leuven
Prof. Laurent Schumacher	UNamur
Dr. Mahdi Sedaghat	Soundness Labs, KU Leuven
Prof. Nigel Smart	KU Leuven, Zama
Prof. François-Xavier Standaert	UCLouvain
Prof. Mathy Vanhoef	KU Leuven
Prof. Dr. Ir. Ingrid Verbauwhede	KU Leuven
Dr. Rafael Gálvez Vizcaíno	KU Leuven
Dr. Iwein Vranckx	Engilico Engineering
Dr. Lennert Wouters	KU Leuven
Dr. Takahito Yoshizawa	KU Leuven

Bulgaria

Prof. Tsonka Baicheva	Bulgarian Academy of Sciences

Canada

Prof. Ian Goldberg	University of Waterloo
Dr. Ryan Henry	University of Calgary

Prof. Bailey Kacsmar	University of Alberta
Prof. Nicolas Papernot	University of Toronto and Vector Institute
Prof. David Murkami Wood	University of Ottawa

Croatia

Prof. Marko Horvat	University of Zagreb
Prof. Stjepan Picek	University of Zagreb, Radboud University

Cyprus

Prof. Elias Athanasopoulos	University of Cyprus

Czechia

Prof. Petr Svenda, Ph.D.	Masaryk University
Prof. Jan Hajny	Brno University of Technology
Dr. Pavel Hubacek	Czech Academy of Sciences, Charles University
Prof. Lukas Malina	Brno University of Technology
Prof. Vashek Matyas	Masaryk University

Denmark

Prof. Diego F. Aranha	Aarhus University
Prof. Aslan Askarov	Aarhus University
Dr. Stein Arne Brekke	University of Copenhagen
Prof. Ivan Damgård	Aarhus University
Prof. Nicola Dragoni	Technical University of Denmark
Prof. Rosario Giustolisi	IT University of Copenhagen

Prof. Christian Majenz	Technical University of Denmark
Prof. Jacopo Mauro	University of Southern Denmark
Prof. Hiraku Morita	University of Southern Denmark
Prof. Ruben Niederhagen	University of Southern Denmark
Prof. Rasmus Løvenstein Olsen	Aalborg University
Prof. Claudio Orlandi	Aarhus University
Prof. Jens Myrup Pedersen	Aalborg University
Prof. Peter Scholl	Aarhus University
Dr. Mark Simkin	Aarhus University
Prof. Luisa Siniscalchi	Technical University of Denmark
Prof. Lene Sorensen	Aalborg University
Prof. Tyge Tiessen	Technical University of Denmark
Prof. Sophia Yakoubov	Aarhus University

Estonia

Dr. Dan Bogdanov	Estonian Academy of Sciences
Dr. Maiara F. Bollauf	University of Tartu
Dr. Ljubov Jaanuska	University of Tartu
Prof. Heiki-Jaan Kaalep	University of Tartu
Dr. Liina Kamm	Cybernetica AS
Dr. Ivan Koppel	University of Tartu
Prof. Helger Lipmaa	University of Tartu
Dr. Chad Nester	University of Tartu
Dr. Arnis Parsovs	University of Tartu
Dr. Janno Siim	University of Tartu

Finland

Prof. Dr. Chris Brzuska	Aalto University
Prof. Kimmo Halunen	University of Oulu
Prof. Camilla Hollanti	Aalto University
Prof. Mikko Kivelä	Aalto University
Prof. Dr. Russell W. F. Lai	Aalto University
Prof. Markku-Juhani O. Saarinen	Tampere University

France

Dr. Marianne Akian	Inria
Prof. David Baelde	Université de Rennes
Dr. Gustavo Banegas	Inria
Dr. Martin Bodin	Inria
Dr. Xavier Bonnetain	Inria
Dr. Daniel De Almeida Braga	Université de Rennes
Dr. Anne Canteaut	Inria
Prof. Rémi Cogranne	Troyes University of Technology
Dr. Alexandre Debant	Inria
Dr. Stéphanie Delaune	CNRS
Dr. Jannik Dreier	Université de Lorraine
Dr. Sébastien Duval	Université de Lorraine
Dr. Benjamin Farinier	Université de Rennes
Dr. Barbara Fila	INSA Rennes
Dr. Caroline Fontaine	CNRS

Aurélien Francillon	EURECOM
Dr. Aymeric Fromherz	Inria
Prof. Joaquin Garcia-Alfaro	Institut Polytechnique de Paris
Dr. Pierrick Gaudry	CNRS
Dr. Georgy Ishmaev	Inria
Dr. Charlie Jacomme	Inria
Dr. Adrien Koutsos	Inria
Dr. Steve Kremer	Inria
Dr. Joseph Lallemand	CNRS
Dr. Pierre Laperdrix	CNRS
Dr. Vincent Laporte	Inria
Dr. Jean-Marc Lasgouttes	Inria
Dr. Gaëtan Leurent	Inria
Dr. Victor Lomne	NinjaLab
Dr. Jean-Marie Madiot	Inria
Dr. Damien Marion	Université de Rennes
Dr. Stephan Merz	Inria
Dr. Raphaël Monat	Inria
Dr. Fabrice Neyret	CNRS
Dr. Andrea Oliveri	EURECOM
Dr. Cristina Onete	Université de Limoges
Dr. Michele Orrù	CNRS
Prof. Lafourcade Pascal	University Clermont Auvergne
Dr. Gwendal Patat	Université de Rennes
Dr. Léo Perrin	Inria

Dr. Virgile Prevosto	Université Paris-Saclay
Dr. Rémi Prébet	Inria, ENS Lyon
Dr. Maxime Puys	Université Clermont Auvergne
Dr. Maïwenn Racouchot	Université Paris-Saclay
Dr. Merve Sahin	Personal capacity
Dr. Guillaume Scerri	ENS Paris Saclay
Dr. Bruno Scherrer	Inria
Dr. Alan Schmitt	Inria
Dr. André Schrottenloher	Inria
Emmanuel Thomé	Inria
Dr. Malisa Vucinic	Inria
Rigo Wenning	GEIE ERCIM
Prof. Melek Önen	EURECOM

Germany

Prof. Dr. Yasemin Acar	Paderborn University
Prof. Dr. Suzana Alpsancar	Paderborn University
Prof. Sebastian Berndt	Technische Hochschule Luebeck
Wasilij Beskorovajnov	FZI Research Center for Computer Science
Dr. Asia Biega	Max Planck Institute for Security and Privacy
Prof. Dr. Kevin Borgolte	Ruhr University Bochum
Prof. Dr. Frank Breitinger	Universität Augsburg
Dr. Sven Bugiel	CISPA Helmholtz Center for Information Security
Prof. Chitchanok Chuengsatiansup	Hasso-Plattner-Institute, University of Potsdam

Prof. Jiska Classen	Hasso-Plattner-Institute, University of Potsdam
Prof. Dr. Cas Cremers	CISPA Helmholtz Center for Information Security
Prof. Dr. Alexandra Dmitrienko	University of Wuerzburg
Prof. Dr. Derek Dreyer	Max Planck Institute for Software Systems
Prof. Dr. Kai Eckert	TH Mannheim
Dr. Kasra Edalatnejad	TU Darmstadt
Prof. Dr.-Ing. Thomas Eisenbarth	University of Lübeck
Prof. Sascha Fahl	CISPA Helmholtz Center for Information Security
Dr.-Ing. Aurore Fass	CISPA Helmholtz Center for Information Security
Prof. Sebastian Faust	TU Darmstadt
Prof. Dr. Felix Freiling	FAU Erlangen-Nürnberg
Prof. Florian Gallwitz	TH Nuremberg
Prof. Dr. Deepak Garg	Max Planck Institute for Software Systems
Dr.-Ing. Kai Gellert	University of Wuppertal
Dr. Maximilian Golla	CISPA Helmholtz Center for Information Security
Prof. Dr.-Ing. Martin Grothe	Niederrhein University of Applied Sciences
Prof. Krishna P. Gummadi	Max Planck Institute for Software Systems
Prof. Dr.-Ing. Tim Güneysu	Ruhr University Bochum
Dr.-Ing. Tobias Handirk	genua GmbH
Prof. Dr. Dominik Herrmann	University of Bamberg
Prof. Matthias Hollick	TU Darmstadt
Prof. Thorsten Holz	Max Planck Institute for Security and Privacy
Prof. Dr. Ralph Holz	University of Münster
Dr. Máté Horváth	University of Wuppertal

Dr. Henry Hosseini	Westphalian University of Applied Sciences, University of Münster
Apl. Prof. Dr. Catalin Hritcu	Max Planck Institute for Security and Privacy
Prof. Dr.-Ing. Luigi Lo Iacono	University of Giessen
Prof. Dr.-Ing. Tibor Jager	University of Wuppertal
Prof. Dr. Martin Johns	TU Braunschweig
Prof. Ghassan Karame	Ruhr University Bochum
Prof. Dr. Stefan Katzenbeisser	University of Passau
Dr. Franziskus Kiefer	Cryspen
Prof. Dr. Eike Kiltz	Ruhr University Bochum
Dr. Michael Klooß	Karlsruhe Institute of Technology
Dr. Konrad Kohbrok	Phoenix R&D
Dr. Katharina Krombholz	CISPA Helmholtz Center for Information Security
Prof. Dr. Klaas Ole Kuertz	Kiel University of Applied Sciences
Dr. Robert Künnemann	CISPA Helmholtz Center for Information Security
Prof. Dr. Anja Lehmann	Hasso-Plattner-Institute, University of Potsdam
Dr. Wouter Lueks	CISPA Helmholtz Center for Information Security
Dr. Lin Lyu	University of Wuppertal
Prof. Dr. Klaus-Peter Löhr	Personal capacity
Prof. Dr. Christian Mainka	University of Wuppertal
Prof. Dr. Karola Marky	Ruhr University Bochum
Ninja Marnau	CISPA Helmholtz Center for Information Security
Prof. Dr.-Ing. Andreas Mayer	Heilbronn University of Applied Sciences
Dr. Jeremias Mechler	Karlsruhe Institute of Technology
Dr. Abraham Mhaidli	Max Planck Institute for Security and Privacy

Prof. Dr.-Ing. Markus Miettinen	Frankfurt University of Applied Sciences
Prof. Dr. Esfandiar Mohammadi	University of Lübeck
Prof. Dr. Veelasha Moonsamy	Ruhr University Bochum
Prof. Amir Moradi	TU Darmstadt
Dr. Christian Mouchet	Hasso-Plattner-Institute, University of Potsdam
Dr. Simon Oberthür	Paderborn University, SICP
Prof. Dr. Rebekah Overdorf	Ruhr University Bochum
Dr. Kentrell Owens	Max Planck Institute for Security and Privacy
Prof. Christof Paar	Max Planck Institute for Security and Privacy
Prof. Dr. Lorenz Panny	Technische Universität München
Dr. Giancarlo Pellegrino	CISPA Helmholtz Center for Information Security
Dr. Daniela Pöhn	Universität der Bundeswehr München
Dr. Willy Quach	CISPA Helmholtz Center for Information Security
Prof. Dr. Kai Rannenberg	Goethe University Frankfurt
Prof. Dr. Dr. Christian Reuter	TU Darmstadt
Prof. Dr. Konrad Rieck	BIFOLD & TU Berlin
Dr. Doreen Riepel	CISPA Helmholtz Center for Information Security
Prof. Dr. Christian Riess	FAU Erlangen-Nürnberg
Prof. Dr. Stefanie Roos	University of Kaiserslautern-Landau
Prof. Christian Rossow	CISPA Helmholtz Center for Information Security
Prof. Paul Rösler	FAU Erlangen-Nürnberg
Dr. Martin Schanzenbach	Fraunhofer Institute for Applied and Integrated Security
Prof. Dr. Sebastian Schinzel	FH Münster, Fraunhofer SIT, Athene National Research Center for Applied Cybersecurity
Prof. Thomas Schneider	TU Darmstadt

Dr. Clara Schneidewind	Max Planck Institute for Security and Privacy
Peter Schoo	Personal capacity
Dr. Matthias Schunter	Intel Labs
Prof. Dr. Peter Schwabe	Max Planck Institute for Security and Privacy, Radboud University
Prof. Jörg Schwenk	Ruhr University Bochum
Dr. Lea Schönherr	CISPA Helmholtz Center for Information Security
Dr. Johannes Schönrich-Sedlmeir	University of Münster
Dr. Henning Seidler	TU Berlin
Prof. Dr. Daniel Slamanig	Universität der Bundeswehr München
Prof. Dr.-Ing. Juraj Somorovsky	Paderborn University
Prof. Dr. Christoph Sorge	Saarland University
Prof. Dr. Indra Spiecker	University of Cologne
Prof. Dr. Barbara Sprick	Technische Hochschule Aschaffenburg
Prof. Dr. Alexander Steen	University of Greifswald
Dr.-Ing. Ben Stock	CISPA Helmholtz Center for Information Security
Prof. Dr.-Ing. Thorsten Strufe	Karlsruhe Institute of Technology
Dr. Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security
Dr.-Ing. Amos Treiber	Personal Capacity
Prof. Carmela Troncoso	Max Planck Institute for Security and Privacy, EPFL
Prof. Dr. Florian Tschorsch	TU Dresden
Prof. Dr. Dominique Unruh	RWTH Aachen University
Prof. Dr. Tobias Urban	Westphalian University of Applied Sciences
Dr. Anjo Vahldiek-Oberwagner	Personal capacity
Dr. Marloes Venema	University of Wuppertal

Dr. Vasilis Ververis	Hasso-Plattner-Institute, University of Potsdam
Prof. Jilles Vreeken	CISPA Helmholtz Center for Information Security
Dr. Théophile Wallez	CISPA Helmholtz Center for Information Security
Prof. Dr. Andreas Westfeld	HTW Dresden
Dr.-Ing. Jan Wichelmann	Universität zu Lübeck
Prof. Dr. Yuval Yarom	Ruhr University Bochum
Dr. Alexandros Zacharakis	Hasso-Plattner-Institute, University of Potsdam
Dr. Xiao Zhang	CISPA Helmholtz Center for Information Security
Prof. Michael Zohner	Hochschule Fulda
Dr. Yixin Zou	Max Planck Institute for Security and Privacy

Greece

Prof. Stefanos Gritzalis	University of Piraeus
Prof. Spyros Kokolakis	University of the Aegean
Dr. Ioannis Krontiris	Ubitech Ltd.
Prof. Panagiotis Rizomiliotis	Harokopio University of Athens
Prof. Georgios Stergiopoulos	Athens University of Economics and Business

Hungary

Dr. Gergely Biczók	Budapest University of Technology and Economics
Prof. Levente Buttyan	Budapest University of Technology and Economics
Dr. Tamás Holczer	BME

Iceland

Prof. Giovanni Apruzzese	University of Reykjavik

Ireland

Dr. Abeba Birhane	Trinity College Dublin
Dr. Ciara Bracken-Roche	Maynooth University
Prof. John G. Breslin	University of Galway
Dr. Róisín Á Costello	Trinity College Dublin
Dr. Stephen Farrell	Trinity College Dublin
Dr. Rónán Kennedy	University of Galway
Prof. Douglas Leith	Trinity College Dublin
Dr. TJ McIntyre	University College Dublin, Digital Rights Ireland
Dr. Harshvardhan Pandit	Trinity College Dublin
Dr. Maria Grazia Porcedda	Trinity College Dublin
Dr. Kris Shrishak	ICCL - Enforce

Israel

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

Italy

Prof. Alessandro Barenghi	Politecnico di Milano
Prof. Stefano Calzavara	Università Ca' Foscari Venezia
Dr. Davide Carnemolla	University of Catania
Prof. Bruno Crispo	University of Trento
Dr. Daniele Cono D'Elia	Sapienza University of Rome

Dr. Marco Giraudo	University of Turin
Prof. Riccardo Lazzeretti	Sapienza University of Rome
Francesco Migliaro	University of Catania
Prof. Gerardo Pelosi	Politecnico di Milano
Prof. Giuseppe Persiano	University of Salerno
Dr. Maura Pintor	University of Cagliari
Prof. Leonardo Querzoni	Sapienza University of Rome
Prof. Daniele Venturi	Sapienza University of Rome
Prof. Stefano Zanero	Politecnico di Milano

Luxembourg

Prof. Gabriele Lenzini	University of Luxembourg
Prof. Dr. Sjouke Mauw	University of Luxembourg
Dr. Peter Roenne	University of Luxembourg
Prof. Dr. Peter Y A Ryan	University of Luxembourg

Norway

Dr. Carlos Cid	Simula UiB
Prof. Kristian Gjøsteen	Norwegian University of Science and Technology
Prof. Danilo Gligoroski	Norwegian University of Science and Technology
Dr. Hans Heum	Norwegian University of Science and Technology
Prof. Tjerand Silde	Norwegian University of Science and Technology
Dr. Mohsen Toorani	University of South-Eastern Norway
Prof. Staal A. Vinterbo	Norwegian University of Science and Technology
Prof. Øyvind Ytrehus	University of Bergen

Dr. Morten Øygarden	Simula UiB

Poland

Prof. Stefan Dziembowski	University of Warsaw

Portugal

Prof. Paulo Azevedo	Universidade do Minho
Prof. Luis Soares Barbosa	Universidade do Minho
Prof. Manuel Barbosa	University of Porto
Prof. Manuel Eduardo Carvalho Duarte Correia	University of Porto
Prof. Kevin Gallagher	NOVA School of Science and Technology
Prof. Francisco Almeida Maia	University of Porto
Prof. Rolando Martins	University of Porto
Prof. Nelma Moreira	University of Porto
Dr. Hugo Pacheco	Universidade do Minho
Prof. Rui Prior	University of Porto
Prof. José Proença	University of Porto
Prof. Nuno Santos	INESC-ID, University of Lisbon
Prof. João Vilela	University of Porto

Slovenia

Prof. Marko Hölbl	University of Maribor
Dr. Boštjan Kežmah	University of Maribor

South Korea

Prof. Sang Kil Cha	KAIST

Spain

Prof. Pino Caballero-Gil	Universidad de La Laguna
Dr. Ignacio Cascudo	IMDEA Software Institute
Prof. Jordi Castella-Roca	Universitat Rovira i Virgili
Prof. Josep Domingo-Ferrer	Universitat Rovira i Virgili
Dr. Luis Bernal Escobedo	University of Murcia
Prof. Jose Maria de Fuentes	University Carlos III of Madrid
Dr. Marco Guarnieri	IMDEA Software Institute
Prof. Jordi Herrera-Joancomarti	Universitat Autonoma de Barcelona
Prof. Javier Lopez	University of Malaga
Prof. Lorena González Manzano	University Carlos III of Madrid
Dr. Pedro Moreno-Sanchez	IMDEA Software Institute
Dr. Antonio Nappa	Zimperium Inc.
Prof. Jose A. Onieva	University of Malaga
Dr. Cristina Perez-Sola	Universitat Autonoma de Barcelona
Dr. Jesus Garcia Rodriguez	University of Murcia
Prof. Dr. Ricardo J. Rodríguez	University of Zaragoza
Dr. Enrique Soriano-Salvador	Universidad Rey Juan Carlos
Prof. Juan Tapiador	University Carlos III of Madrid
Prof. Maria Isabel Gonzalez Vasco	University Carlos III of Madrid
Dr. Niki Vazou	IMDEA Software Institute

Sweden

Dr. Simon Bouget	RISE Research Institutes of Sweden
Dr. Christoph Egger	Chalmers University of Technology
Dr. Lars-Henrik Eriksson	Uppsala University
Alfonso Iacovazzi	RISE Research Institutes of Sweden
Prof. Dr.-Ing. Meiko Jensen	Karlstad University
Dr. Adrian PErez Keilty	Chalmers University
Dr. Victor Morel	Chalmers University of Technology
Elena Pagnin	Chalmers University of Technology and University of Gothenburg
Dr. Justin Pearson	Uppsala University
Dr. Tobias Pulls	Karlstad University
Dr. Apostolos Pyrgelis	RISE Research Institutes of Sweden
Dr. Iraklis Symeonidis	Personal capacity
Dr. Marco Tiloca	RISE Research Institutes of Sweden
Prof. Bjorn Victor	Uppsala University

Switzerland

Prof. David Basin	ETH Zurich
Dr. Andrea Basso	IBM Research
Dr. Ward Beullens	IBM Research
Prof. Dr. Srdjan Capkun	ETH Zurich
Dr. Ana-Maria Cretu	EPFL
Dr. Elizabeth Crites	Web3 Foundation

Prof. Jean-Pierre Hubaux	EPFL
Frederic Jacobs	Personal capacity
Dr. Pascal Junod	Personal capacity
Dr. Anil Kurmus	IBM Research
Dr. Simon-Philipp Merz	ETH Zurich
Prof. Kenneth Paterson	ETH Zurich
Prof. Mathias Payer	EPFL
Prof. Adrian Perrig	ETH Zurich
Dr. Benjamin Rothenberger	Zühlke
Dr. Ralf Sasse	ETH Zurich
Dr. Theresa Stadler	EPFL
Dr. Piet De Vaere	ETH Zurich
Prof. Isabel Wagner	University of Basel

Taiwan

Dr. Matthias Kannwischer	Chelpis Quantum Corp

The Netherlands

Dr. Gunes Acar	Radboud University
Prof. Luca Allodi	Eindhoven University of Technology
Prof. Lejla Batina	Radboud University
Prof.Dr. Bibi van den Berg	Leiden University
Prof. Jeanne Mifsud Bonnici	University of Groningen
Prof. Dr. Frederik Zuiderveen Borgesius	Radboud University

Prof. Dr. Herbert Bos	VU Amsterdam
Dr. Ir. Xavier de Carné de Carnavalet	Radboud University
Prof. Andrea Continella	University of Twente
Dr. Lorenzo Dalla Corte	Tilburg Institute for Law, Technology and Society
Prof. Ronald Cramer	CWI, Leiden University
Prof. Joan Daemen	Radboud University
Prof. Marten van Dijk	CWI
Prof.Dr. Michel van Eeten	TU Delft
Dr. Zeki Erkin	TU Delft
Prof. Cristiano Giuffrida	VU Amsterdam
Dr. Seda Gürses	TU Delft
Dr.-Ing. Florian Hahn	University of Twente
Prof. Dr. Jaap-Henk Hoepman	Radboud University, Karlstad University
Dr. Andreas Hülsing	Eindhoven University of Technology
Prof. Bart Jacobs	Radboud University
Dr. Slinger Jansen	Utrecht University
Dr. Konrad Kollnig	Maastricht University
Dr. ing. Ralph Koning	University of Amsterdam
Prof. Bert-Jaap Koops	Tilburg University
Prof. Dr. Tanja Lange	Eindhoven University of Technology
Prof.Dr. Ronald Leenes	Tilburg University
Prof. Eleftheria Makri	Leiden University
Dr. Luca Mariot	University of Twente
Prof. Bart Mennink	Maastricht University

Prof. Dr. Lokke Moerel	Tilburg University
Dr. Giovane Moura	TU Delft
Dr. Subhasree Patro	Eindhoven University of Technology
Dr. Paola de Perthuis	CWI
Dr.ir. Erik Poll	Radboud University
Prof. Dr. ir. Roland van Rijswijk-Deij	University of Twente
Prof. Simona Samardjiska	Radboud University
Prof. Christian Schaffner	University of Amsterdam
Dr. Theodor Schnitzler	Maastricht University
Dr. Hanna Schraffenberger	Radboud University
Prof. Monika Trimoska	Eindhoven University of Technology
Dr. Christine Utz	Radboud University
Dr. Heloise Vieira	Eindhoven University of Technology
Dr. Jeroen van der Ham-de Vos	University of Twente
Dr. Thom Wiggers	Personal capacity
Dr. Mengyuan Zhang	VU Amsterdam

Turkey

Prof. Cihangir Tezcan	Middle East Technical University

United Arab Emirates

Prof. Mihalis Maniatakos	New York University Abu Dhabi
Prof. Christina Poepper	New York University Abu Dhabi

United Kingdom

Prof. Martin Albrecht	King's College London
Dr. Panagiotis Andriotis	University of Birmingham
Prof. Eerke Boiten	De Montfort University
Prof. Ioana Boureanu	University of Surrey
Dr. Giovanni Cherubin	Microsoft Research
Prof. Nathan Clarke	University of Plymouth
Dr. Simone Colombo	King’s College London
Dr. François Dupressoir	University of Bristol
Prof. Elaine Fahey	City St. Georges, University of London
Dr. Joël Felderhoff	King's College London
Honorary Prof. Jens Groth	Nexus, University College London
Dr. Neil Hanley	Queens University Belfast
Prof. Alice Hutchings	University of Cambridge
Dr. Dennis Jackson	Mozilla
Prof. Rikke Bjerg Jensen	Royal Holloway, University of London
Prof. Vasilis Katos	Bournemouth University
Prof. Markulf Kohlweiss	University of Edinburgh
Dr. Kaspar Rosager Ludvigsen	Durham University
Prof. Keith Martin	Royal Holloway, University of London
Prof. Andrew Martin	University of Oxford
Prof. Sarah Meiklejohn	University College London
Prof. Andy Phippen	Bournemouth University
Dr. Eamonn Postlethwaite	King's College London
Prof. Kasper Rasmussen	University of Oxford

Prof. Steve Schneider	University of Surrey
Dr. Fernando Virdia	University of Surrey
Dr. Christian Weinert	Royal Holloway, University of London

United States of America

Prof. Antonio Bianchi	Purdue University
Prof. L Jean Camp	Indiana University
Dr. Daniel Collins	New York University, Hebrew University
Prof. Christina Garman	Purdue University
Prof. Matthew D. Green	Johns Hopkins University
Prof. Paul Grubbs	University of Michigan
Prof. Vasileios Kemerlis	Brown University
Prof. Susan Landau	Tufts University
Prof. Anna Lysyanskaya	Brown University
Prof. Michelle Mazurek	University of Maryland
Prof. Michalis Polychronakis	Stony Brook University
Dr. Niels Provos	Security Blueprints, LLC
Prof. Amir Rahmati	Stony Brook University
Prof. Aanjhan Ranganathan	Northeastern University / ETH Zürich
Prof. Nitesh Saxena	Texas A&M University
Prof. Adam Shostack	Personal Capacity
Dr. Alin Tomescu	Aptos Labs
Prof. Blase Ur	University of Chicago
Prof. Chau-Wai Wong	North Carolina State University
Prof. Daniel Zappala	Brigham Young University