Joint statement of security and privacy scientists and researchers on Age Assurance
Executive summary

We are writing in response to the worldwide initiatives to introduce age assurance technologies to implement access control to internet services. We share the concerns about the negative effects that exposure to harmful content online has on children, and we applaud that regulators dedicate time and effort to protect them. However, we fear that, if implemented without careful consideration of the technological hazards and societal impact, the new regulation might cause more harm than good.

Age-based regulations have existed in the offline world for a long time: to prevent minors from entering casinos, buying alcohol, or accessing adult content. These checks are based on existing ID documents, only require an existing employee checking the document, and rarely leave written records. The current proposals for age assurance online go much further than this limited set of scenarios. More critically, they lack the inherent privacy provided by ID document-based checks offline. Current discussions regarding the need for regulating social media, AI chatbots, or instant messaging would require all users – minors and adults – to prove their age to converse with friends and family, read news, or search for information; well beyond what has ever happened in our offline lives. In addition, access to content and communications platforms also has documented benefits for children and adults to find information, seek advice, and encounter communities to break isolation. We observe with great concern that the introduction of age assurance threatens to eliminate all these benefits without any guarantee that such a measure would be the solution to the harms that worry us all, while at the same time establishing an infrastructure that could be exploited to ban access to Internet services for reasons unrelated to safety.

Age-assurance checks are easy to bypass, as evidenced by current deployments being circumvented using VPNs, bought or borrowed credentials, or props or AI-based tools (e.g., deepfakes or AI-generated profiles), to change the users' appearance. Such checks also require the creation of Internet-wide trust infrastructures that do not exist today, whose technical deployment would be quite complex, and whose worldwide legal enforcement seems doubtful. They are not guaranteed to prevent minors from accessing harmful online content, or adults from entering children-specific spaces designed to be safe.

Age-assurance checks not only might be ineffective, but can actually diminish safety online by exposing users to malware and scams when they resort to alternative services that do not implement verification—and users will undoubtedly turn to such alternative sources. This policy will inevitably massively reduce privacy online by forcing users to reveal more information to service providers than they do nowadays, or lead to limitations on the use of protective technologies such as VPNs. Both create security risks. Safeguarding privacy requires the use of certified age attributes, which requires users to have such a certification, a compatible device, and digital skills to prove their age. These requirements are not met by a significant portion of the population, such as the elderly, non-EU citizens (if age verification is based on upcoming EUDI), anybody who doesn't hold a national digital ID credential, or simply those who do not want to own a smartphone (especially one supported by the verification system). Thus, age-assurance has great potential to increase inequality and discrimination in the digital sphere.

We are writing this letter to call for a moratorium on deployment plans until the scientific consensus settles on the benefits and harms that age-assurance technologies can bring, and on the technical feasibility of such a deployment. Two critical issues have not been addressed: whether age assurance is efficacious and what the potential damages to general security and privacy are. We believe that it is dangerous and socially unacceptable to introduce a large-scale access control mechanism without a clear understanding of the implications that different design decisions can have on security, privacy, equality, and ultimately on the freedom of decision and autonomy of individuals and nations.

Joint statement of security and privacy scientists and researchers on Age Assurance

March 2, 2026

In the following, we use the term age assurance technologies to encompass *age verification* -- where users have proof of identity provided by a trusted party such as a government ID, *age estimation* -- where verifiers use images or video to estimate age using biometric information, and age inference -- where age is estimated from online behaviour, for example, browsing history.

Open questions on the feasibility of effective deployment. For age-based access control to succeed at reducing harm, it needs to be possible to implement it securely and at internet-scale. While the public discussion centers mostly on privacy, there are other important technical considerations that have not received sufficient scrutiny.

Effective deployment is subject to trade-offs. Implementing age assurance effectively is a complex, intricate, and multifaceted problem. A weak implementation would enable minors to access content that is deemed not age-appropriate, and also enable adults to access children-oriented spaces (like Roblox age-group chats), effectively negating the benefits of age-based controls. Overcoming the complex technical challenges outlined below is likely to require compromises and trade-offs that should be analyzed and publicly discussed before launching a ubiquitous intervention at the core of our digital space that, once deployed, would be close to impossible to change.

Age assurance checks can be easily circumvented. The effectiveness of age assessment as a protection measure hinges on three factors: (i) users' inability to acquire tools or credentials that enable them to lie about their age, (ii) users' inability to access alternative services that do not perform age assessment, (iii) access to services is forced through the verification mechanism, and (iv) the accuracy of the the age assessment technology.

There is ample evidence from existing deployments that lying about age is not hard. It can be as easy as using age-verified accounts borrowed from an elder sibling or friend. In fact, there are reported cases of parents helping their children with age circumvention. There is evidence that, shortly after age-based controls appear, markets and services that sell valid accounts or credentials quickly arise. This enables the use of online services deploying age assurance at an affordable price or even for free. This is the case even if the verification is based on government-issued certificates, as shown by the ease with which fake vaccination certificates could be acquired during the COVID pandemic.

Even if users cannot obtain credentials, it is trivial to install a VPN to access services from a jurisdiction without age control requirements or that has different age limits. This is an already widely used practice that is expected to grow as more alternatives appear. Tools are not only limited to geolocated-based circumvention, but we also see how resources to help users deactivate checks to access the service without the need for assurance appear quickly after checks are deployed.

The wide range of circumvention mechanisms available online is a symptom of a mismatch in the threat model associated with age assurance. As its main goal is to restrict the activities of children, it is common to believe that the only adversary is minors trying to bypass age verification. Yet, age verification mechanisms also apply to adults that will have to prove their age in many of their routine online interactions, to access services or to keep them away from children-specific web spaces. As these checks will jeopardize their online experience, adults will have incentives to create means to bypass them both

for their own use or to monetize the bypass. Thus, it is foreseeable that an increase in the deployment of age assurance will result in growing availability of circumvention mechanisms, reducing its effectiveness.

Age estimation and age inference bring harm to users without effectiveness guarantees. To be effective, age assurance needs to work for a wide variety of users and devices. For example, it cannot assume the existence of an app on a smartphone: many users, in particular minors, access the internet from shared computers. Therefore, age estimation and age inference are being deployed alongside age verification (e.g., Discord, Roblox, or ChatGPT). Age estimation and age inference technologies are highly privacy-invasive. They rely on the collection and processing of sensitive, private data such as biometrics, or behavioural or contextual information (e.g., language use). Therefore, deploying these age assurance methods at a large scale facilitates (children's) data collection and exploitation.

Moreover, these technologies are well-known to be unreliable. Age estimation and inference rely mostly on AI-based inferences, which, for the particular data types used to do age-related checks (e.g., biometrics), are known to have high error rates and to be biased for certain minorities. Users can even force errors on these technologies, e.g., by using photos or props like a beard or a moustache. We conclude that age assessment presents an inherent disproportionate risk of serious privacy violations and discrimination, without guarantees of effectiveness.

Building a global trust infrastructure for age verification is non-trivial. For age assurance checks to actually become effective, services would need to implement methods that are difficult to bypass for the majority of users. With the current state-of-the-art, this undoubtedly requires age verification based on government-issued IDs with strong cryptographic protection *for every single interaction with the service*. This would result in poor usability and exclusion of all users without such IDs. Many service providers are unlikely to accept this direction and the resulting loss of business resulting in reduced overall protection.

Moreover, age verification based on a proof of identity is not only error-prone, but requires the existence of a trust infrastructure at Internet scale. This is needed so that any provider deploying age checks can verify age certificates from all users. Building such an infrastructure is not trivial. It requires, among others, establishing trusted issuers equipped to provide digital certificates at large scale, establishing means to provide verifiers with issuer's key material to carry out the verification, and establishing means to revoke certificates. Building such an infrastructure for securing HTTP web traffic took decades. It is not clear how this could be deployed in the short term at world-scale in such a way that services are protected across jurisdictions, and that no users are left without access to services when outside of their nations (e.g., expats, tourists, or business travellers). The EUDI Wallet promises to solve some of these challenges at the European level, yet the infrastructure has not been rolled out, revocation has not yet been resolved, and interoperability beyond the European Union has not been tackled. Finally, as noted above, even if such a trust infrastructure would exist, checks can be circumvented by acquiring valid certificates or using VPNs, as long as age assurance regulations are not universally enforced by all affected services.

Lack of understanding of harms. The public discourse assumes that age-based access control to online services will greatly increase the safety of minors online. Yet, there is no discussion on the harms that such controls could cause to both minors and adults.

Diminish online safety. Deplatforming has been repeatedly shown not to deter users from carrying out an activity. Instead, they migrate to another platform where they can continue their activities. If minors or adults are deplatformed via age-related bans, they are likely to migrate to find similar services. Since the main platforms would all be regulated, it is likely that they would migrate to fringe sites that escape regulation. This would not only negate any benefit of the age-based controls but also expose users to other dangers, such as scams or malware that are monitored in mainstream platforms but exist on smaller providers. Even if users do not move platforms, attempting circumvention to access mainstream services from a jurisdiction that does not mandate age assurance might also increase their risk. For example, free VPN providers might not follow secure practices or might monetize users' data (especially non-EU providers that are not subject to data protection obligations), and websites accessed in other jurisdictions through VPNs would not provide the user with the data protection standards and rights which are guaranteed in the EU.

Moreover, the ease of circumvention risks creating a *false sense of security*. The promise of children-specific services that serve as safe spaces is unrealizable with current technology. This means that children might become exposed to predators who infiltrate these spaces, either via circumvention or acquisition of false credentials that allow them to pose as minors in a verifiable way.

Diminishing privacy online. The mandate to implement age assurance justifies new forms of data collection by online services, especially for age estimation and age inference. This in itself increases privacy risks, with data being potentially abused by the provider itself or its subcontractors, or third parties that get access to it, e.g., after a data breach, like the 70K users that had their government ID photos leaked after appealing age assessment errors on Discord.

Besides direct leakage, age assurance might affect privacy by reducing users' access to privacy technologies. A main circumvention mechanism is the use of VPNs to access services. This has prompted some policymakers to consider the regulation of VPNs, which are essential digital security tools. Regulating the use of VPNs, or subjecting their use to age assurance controls, will decrease the capability of users to defend their privacy online. This will not only force regular users to leave a larger footprint on the network, but will leave a number of at-risk populations unprotected, such as journalists, activists, or domestic abuse victims. It can also potentially hurt the operations of businesses or educational institutions by hindering the use of VPNs for securing remote access to their infrastructure. We note that we do not believe that trying to regulate VPN use for non-compliant users would be any more effective than trying to forbid the use of end-to-end encrypted communication for criminals. Secure cryptography is widely available and can no longer be put back into a box.

Increasing discrimination. Conditioning the access to services on having proof of age means that many adults would not be able to use those services. For example, adults without access to proof of age could be adults without the literacy to use a proof of age such as elderly users; visitors from countries that are not part of the trusted infrastructure; undocumented immigrants, asylum seekers, or incarcerated people. Also users without access to devices, such as those without economic means to acquire one; or users without IDs as a result of being too young, not being able to afford one, or not wanting one. If age assurance checks are introduced, these subgroups would be left behind, or be forced to use either non-private alternatives increasing their risks online or potentially insecure circumvention mechanisms to be able to have a normal digital life.

Introducing legacy infrastructure. Many of the age-based control projects we see nowadays are precursors of, or coupled with, the introduction of a larger identity infrastructure. Such infrastructures are intended to enable the verification of attributes beyond age. Running these verification services will collect

increasing amounts of data, introducing further risks regarding tracking and profiling. And because more services will implement checks, inequality and discrimination will increase as well. Studying age-verification in isolation can result in an underestimation of its potential long-term consequences on the security, privacy, and safety of the Internet.

Centralization of power. Those deciding which age-based controls need to exist, and those enforcing them gain a tremendous influence on what content is accessible to whom on the internet. Recall that age assurance checks might go well beyond what is regulated in the offline world and set up an infrastructure to enforce arbitrary attribute-based policies online. In the wrong hands, such as an authoritarian government, this influence could be used to censor information and prevent users from accessing services, for example, preventing access to LGBTQ+ content. Centralizing access to the internet easily leads to internet shutdowns, as seen recently in Iran. If enforcement happens at the browser or operating system level, the manufacturers of this software would gain even more control to make decisions on what content is accessible on the Internet. This would enable primarily big American companies to control European citizens' access to the internet.

More generally, the centralization of decision-making, as imposed by age assurance-related regulations, is contrary to the end-to-end principle, core to the Internet design. This principle states that application decisions, in particular those security-oriented, should reside on the endpoints. Age assurance, by design, imposes access control rules on those endpoints, threatening the decentralization of the Internet and jeopardizing the creation of sovereign technology.

Lack of discussion of the Privacy Enhancing Technologies (PETs) impact. Privacy concerns and potential solutions are a central part of the discussion, which has led to many proposals for PETs as a solution. We recognize that the tracking capability of a naive implementation of age assurance could be disastrous for privacy and create huge harms. We applaud the effort that is being put into integrating privacy technologies to alleviate these risks. Yet, removing privacy concerns does not address many of the harms that we mention. More generally, the use of PETs risks to bolster centralization by pushing users towards mainstream phone manufacturers that amass more power on the market.

Depending on the implementation, the introduction of PETs might exacerbate existing problems. For example, PETs might bolster discrimination if only some (smart)phones have the necessary capability, software, firmware, or hardware. Users of devices without the required hardware or using operating systems that do not support the necessary functions will be prevented from accessing systems. These are mostly open devices and operating systems, which are mainly favoured by privacy- and security-conscious users. These users would be forced to switch to mainstream devices and software, reducing their protection online.

Moreover, when PETs require complex cryptographic protocols, likely only a few—potentially even a single—implementation will be available, often provided by a single party or company (e.g., Apple or Google). Entities that merely integrate these libraries typically have very limited control over the functionalities provided. Therefore, any changes to the technology must be either made or supported by the supplying party, creating an unresolvable dependency. This not only creates a single point of failure but also immense centralization of power on those controlling the cryptographic libraries.

When privacy requirements are underspecified, and data protection agencies fail to provide explicit regulatory positioning, it creates a dangerous architectural ambiguity that frequently leads to severe data incidents. For example, if a foundational concept such as "unlinkability" can be interpreted loosely, e.g.,

ensuring only that external verifiers cannot link transactions (letting the central authority often retain a complete, global view of user activity), as opposed to the traditional security meaning, where it means that no entity, including the system authority can connect the data points. In the absence of a strong regulation mandating the strict interpretation, organizations naturally default to easier, centralized implementations under the guise of compliance. This compromise creates a massive single point of failure; if that central authority is breached, subpoenaed, or acts maliciously, the supposedly "private" system is completely exposed, transforming a vague technical requirement into a systemic privacy disaster.

Deployment is not justified unless it is proven that the benefits greatly outweigh the harms. Beyond technical issues, there is no scientific evidence to support the assumption that banning minors from accessing services would have a positive effect on their mental health and development. Given the potential risks and available alternatives, deploying a technology with such wide impact without understanding its implications for the online security and privacy of individuals, communities, and societies *cannot be called a proportional solution*.

If children and adults are to be protected from harm, it is of utmost importance that an in-depth study of the harms and broader consequences of age-based checks is conducted before mandating this technology at Internet-scale. Deployments in the UK or Australia, and the introduction of age checks by main providers calls for systematically studying the benefits and harms of this technological intervention.

In the meantime, we encourage the exploration of alternative measures, especially those that tackle the root of the harm. Many of the harms that age-based checks are supposed to address are caused by algorithmic practices of social networks; hence, regulating those practices to prevent users from being exposed to harmful content would be more directly effective than circumventable access control checks, and would also promote safer services for children and adults. Other avenues to explore include dedicating resources to improve the support for parents to locally prevent access to non-age-appropriate content or apps, without age-based control needing to be implemented by service providers.

Signatories **(affiliations are for identification purposes only)**

Austria

Prof. Daniel Gruss	Graz University of Technology
Dr. Walter Hötzendorfer	Research Institute – Digital Human Rights Center
Dr. Christoph Kerschbaumer	Mozilla
Prof. Dr. Martina Lindorfer	TU Wien
Prof. Dr. Matteo Maffei	TU Wien
Prof. René Mayrhofer	Johannes Kepler University Linz

Dr. Peter Pfeiffer	Johannes Kepler University Linz
Prof. Krzysztof Pietrzak	Institute of Science and Technology Austria
Prof. Christian Rechberger	Graz University of Technology
Dr. Michael Roland	Johannes Kepler University Linz
Prof. Sujoy Sinha Roy	Graz University of Technology
Dr. Johannes Sametinger	Johannes Kepler University Linz
Prof. Dominique Schröder	TU Wien
Prof. Edgar Weippl	University of Vienna

Belgium

Dr. Aysajan Abidin	KU Leuven
Dr. Emad Heydari Beni	KU Leuven
Dr. Rachelle Heim Boissier	Université Libre de Bruxelles
Dr. Rosamunde Van Brakel	Vrije Universiteit Brussel
Dr. Gaetan Cassiers	UCLouvain
Prof. Bart Coppens	Ghent University
Prof. Geert Deconinck	KU Leuven
Dr. Thomas Decru	KU Leuven
Prof. Claudia Diaz	KU Leuven
Prof. Denis Flandre	UCLouvain
Dr. Gertjan Franken	KU Leuven
Dr. Rafa Galvez	KU Leuven
Dr. Mariana Gama	KU Leuven
Dr. Benedikt Gierlichs	KU Leuven
Dr. Milos Grujic	KU Leuven

Dr. Francois Koeune	UCLouvain
Dr. Jorn Lapon	KU Leuven
Prof. Dr. Yunwen Liu	KU Leuven
Dr. Hannes Mareen	Ghent University
Dr. Thorben Moos	UCLouvain
Prof. Yves Moreau	KU Leuven
Prof. Jan Tobias Muehlberg	Universite Libre de Bruxelles
Dr. Roel Peeters	KU Leuven
Prof. Olivier Pereira	UCLouvain
Prof. Thomas Peters	UCLouvain
Prof. Jo Pierson	Hasselt University
Prof. Bart Preneel	KU Leuven
Prof. Jean Jacques Quisquater	UCLouvain
Prof. Florentin Rochet	UNamur
Prof. Sofie Royer	Vrije Universiteit Brussel, KU Leuven
Prof. Wim Schoutens	KU Leuven
Prof. Dr. Ir. Dave Singelee	KU Leuven
Prof. François-Xavier Standaert	UCLouvain
Prof. Dr. Mathy Vanhoef	KU Leuven
Paola Verhaert	Independent
Dr. Iwein Vranckx	Engilico Engineering
Prof. Cato Waeterloos	Hasselt University

Canada

Prof. Ian Goldberg	University of Waterloo

Prof. Ryan Henry	University of Calgary
Prof. Bailey Kacsmar	University of Alberta
Prof. Michael Karanicolas	Dalhousie University
Prof. Simon Oya	The University of British Columbia
Prof. Nicolas Papernot	University of Toronto and Vector Institute

Croatia

Prof. Tajana Ban Kirigin	University of Rijeka

Czech Republic

Dr. Pavel Hubacek	Czech Academy of Sciences and Charles University
Prof. Petr Svenda	Masaryk University

Denmark

Prof. Diego F. Aranha	Aarhus University
Prof. James Avery	University of Copenhagen
Prof. Ivan Damgård	Aarhus University
Dr. Laouen Fernet	University of Copenhagen
Prof. Andrzej Filinski	University of Copenhagen
Prof. Fritz Henglein	University of Copenhagen
Prof. Thore Husfeldt	IT University of Copenhagen
Dr. Jiang	University of Copenhagen
Dr. David Marchant	University of Copenhagen
Dr. Boel Nelson	University of Copenhagen
Prof. Rasmus Pagh	University of Copenhagen

Prof. Jens Myrup Pedersen	Aalborg University
Prof. Peter Scholl	Aarhus University
Prof. Luisa Siniscalchi	Technical University of Denmark

Estonia

Dr. Dan Bogdanov	Estonian Academy of Sciences
Prof. Helger Lipmaa	University of Tartu
Dr. Janno Siim	University of Tartu

Finland

Prof. Kimmo Halunen	University of Oulu
Dr. Mikko Heikkilä	University of Helsinki
Prof. Antti Honkela	University of Helsinki
Prof. Russell W. F. Lai	Aalto University
Prof. Antonis Michalas	Tampere University
Prof. Sebastian Szyller	Aalto University

France

Dr. Gustavo Banegas	Inria
Dr. Gabrielle Beck	CNRS, University of Montpellier
Prof. Olivier Blazy	Ecole polytechnique
Dr. Xavier Bonnetain	Inria
Dr. Anne Canteaut	Inria
Prof. Anne Cordier	Université de Lorraine
Dr. Sébastien Duval	Université de Lorraine

Prof. Severine Erhel	Université Rennes 2
Prof. Aurélien Francillon	EURECOM
Dr. Aymeric Fromherz	Inria
Prof. Joaquin Garcia-Alfaro	Institut Polytechnique de Paris
Dr. Bruno Grenet	Université Grenoble Alpes
Prof. Phan Duong Hieu	Télécom Paris, Institut Polytechnique de Paris
Dr. Charlie Jacomme	Inria
Dr. Christophe Kiennert	Institut Polytechnique de Paris
Dr. Nadim Kobeissi	Symbolic Software
Dr. Adrien Koutsos	Inria
Prof. Pascal Lafourcade	Université Clermont Auvergne
Dr. Eran Lambooij	Inria
Dr. Pierre Laperdrix	CNRS
Dr. Vincent Laporte	Inria
Dr. Gaëtan Leurent	Inria
Dr. Damien Marion	Université de Rennes
Dr. Stephan Merz	Inria
Dr. Francesco Migliaro	CNRS, Université Paris Cité
Dr. Raphaël Monat	Inria
Dr. Ing. Renzo E. Navas	IMT Atlantique
Dr. Andrea Oliveri	EURECOM
Dr. Charles Olivier-Anclin	Université Clermont Auvergne
Dr. Melek Onen	EURECOM
Dr. Cristina Onete	University of Limoges
Dr. Gwendal Patat	Université de Rennes

Dr. Leo Perrin	Inria
Dr. Pierrick Philippe	Inria
Dr. Thomas Prevost	Universite Clermont Auvergne
Dr. Maxime Puys	Université Clermont Auvergne
Dr. Samuel Pélissier	CentraleSupélec
Dr. Yann Rotella	Université Paris-Saclay
Dr. Merve Sahin	Personal capacity
Dr. Jean-Pierre Tillich	Inria
Dr. Suzanne Vergnolle	Conservatoire national des arts et métiers
Dr. Yingfei Yan	Université Clermont Auvergne

Germany

Prof. Dr. Florian Adamsky	Hof University of Applied Sciences
Dr. Steffen Becker	Ruhr University Bochum
Prof. Sebastian Berndt	Technische Hochschule Lübeck
Dr. Roland Bless	Karlsruhe Institute of Technology
Prof. Dr. Kevin Borgolte	Ruhr University Bochum
Prof. Frank Breitinger	University of Augsburg
Dr. Gianluca Brian	TU Darmstadt
Prof. Joanna J. Bryson	Hertie School of Governance
Prof. Andreas Bulling	University of Stuttgart
Prof. Dr. Jiska Classen	University of Potsdam
Dr. Ana-Maria Cretu	CISPA Helmholtz Center for Information Security
Dr. Daniel Demmler	Zama
Dr. Guillaume Didier	Saarland University

Prof. Derek Dreyer	MPI-SWS
Prof. Dr. Kai Eckert	Mannheim Technical University of Applied Sciences
Dr. Kasra Edalatnejad	TU Darmstadt
Prof. Dr. Matthias Faes	TU Dortmund
Prof. Dr. Mathias Fischer	University of Hamburg
Dr. Kai Gellert	University of Wuppertal
Dr. Maximilian Golla	CISPA Helmholtz Center for Information Security
Dr. Marc Gourjon	MPI-SP
Dr.-Ing. Dominik Helm	University of Stuttgart
Prof. Dr. Dominik Herrmann	Otto-Friedrich-Universität Bamberg
Prof. Matthias Hollick	TU Darmstadt
Prof. Thorsten Holz	MPI-SP
Dr. Máté Horváth	University of Wuppertal
Dr. Henry Hosseini	Westphalian University of Applied Sciences, University of Münster
Prof. Dr. Luigi Lo Iacono	University of Giessen
Prof. Tibor Jager	University of Wuppertal
Prof. Dr. Stefan Katzenbeisser	University of Passau
Dr. Franziskus Kiefer	Cryspen
Dr. Michael Klooß	Karlsruhe Institute of Technology
Dr. Georg Land	Personal capacity
Prof. Anja Lehmann	University of Potsdam
Dr. Wouter Lueks	CISPA Helmholtz Center for Information Security
Dr. Adrian Marotzke	Personal capacity
Prof. Dr. Andreas Mayer	Heilbronn University of Applied Sciences

Dr. Sebastian Meiser	Universität zu Lübeck
Dr. Abraham Mhaidli	MPI-SP
Dr. Tamalika Mukherjee	MPI-SP
Prof. Dr. Rebekah Overdorf	Ruhr University Bochum
Prof. Dr. Lorenz Panny	TU München
Dr. Sebastian Pape	Goethe University Frankfurt
Prof. Dr. Joachim Posegga	University of Passau
Prof. Dr. Konrad Rieck	BIFOLD & TU Berlin
Dr. Doreen Riepel	CISPA Helmholtz Center for Information Security
Dr.-Ing. Tim Ruffing	Blockstream Research
Prof. Dr. Christoph Saatjohann	FH Münster University of Applied Science
Dr. Sajin Sasy	CISPA Helmholtz Center for Information Security
Tim Philipp Schafers	FHDW Paderborn
Dr. Martin Schanzenbach	Fraunhofer AISEC
Dr. Tim Schatto-Eckrodt	University of Hamburg
Prof. Thomas Schneider	TU Darmstadt
Prof. Dr. Thomas Schreck	Munich University of Applied Sciences
Prof. Dr. Stephan Schulz	DHBW Stuttgart
Dr. Matthias Schunter	Intel Labs Europe
Prof. Dr. Peter Schwabe	MPI-SP, Radboud University
Prof. Dr. Jörg Schwenk	Ruhr University Bochum
Dr. Johannes Schönrich-Sedlmeir	University of Münster
Prof. Daniel Slamanig	Universität der Bundeswehr München
Prof. Dr. Christoph Sorge	Saarland University
Dr. Aleksandra Sowa	LK FG PET, GI

Dr.-Ing. Ben Stock	CISPA Helmholtz Center for Information Security
Prof. Dr. Thorsten Strufe	Karlsruhe Institute of Technology
Prof. Carmela Troncoso	MPI-SP, EPFL
Prof. Dr. Dominique Unruh	RWTH Aachen and University of Tartu
Prof. Dr. Tobias Urban	Institute for Internet Security; Westphalian University of Applied Sciences
Dr. Anjo Vahldiek-Oberwagner	Personal capacity
Dr. Marloes Venema	University of Wuppertal
Prof. Markus Wamser	Technische Hochschule Ingolstadt
Prof. Dr. Yuval Yarom	Ruhr University Bochum
Dr. Yixin Zou	MPI-SP

Greece

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

Hungary

Dr. Gergely Biczók	Budapest University of Technology and Economics
Dr. Tamás Holczer	BME
Dr. Balazs Pejo	Budapest University of Technology and Economics
Dr. István András Seres	Eötvös Loránd University

Iceland

Prof. Giovanni Apruzzese	Reykjavik University

Ireland

Dr. Abeba Birhane	Trinity College Dublin
Dr. Stephen Farrell	Trinity College Dublin
Dr. Ronan Kennedy	University of Galway
Prof. Douglas Leith	Trinity College Dublin
Prof. David Malone	Maynooth University
Dr. TJ McIntyre	University College Dublin
Dr. Pauline Meyer	Trinity College Dublin
Prof. Eoin O'Dell	Trinity College Dublin
Dr. Maria Grazia Porcedda	Trinity College Dublin
Dr. Kris Shrishak	ICCL - Enforce
Prof. John Stalker	Trinity College Dublin

Israel

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

Italy

Prof. Marco Baldi	Università Politecnica delle Marche
Prof. Alessandro Barenghi	Politecnico di Milano
Prof. Federica Capeplluti	Politecnico di Torino

Prof. Mauro Conti	University of Padua, Örebro University
Prof. Giorgio Giacinto	University of Cagliari
Prof. Riccardo Lazzeretti	Sapienza University of Rome
Dr. Lorenzo Magliocco	Personal capacity
Prof. Emmanuela Orsini	Bocconi University
Dr. Maria Antonietta Pascali	National Research Council
Prof. Gerardo Pelosi	Politecnico di Milano
Dr. Simone Perriello	Politecnico di Milano
Prof. Giuseppe Persiano	Università di Salerno
Andrea Reale	Sapienza University of Rome
Dr. Leonardo Regano	Università degli Studi di Cagliari
Prof. Antonio J. Di Scala	Politecnico di Torino
Prof. Marco Torchiano	Politecnico di Torino
Prof. Stefano Zanero	Politecnico di Milano

Luxembourg

Prof. Sjouke Mauw	University of Luxembourg
Prof. Peter Y A Ryan	University of Luxembourg
Dr. Felix Stutz	University of Luxembourg
Dr. Aleksei Udovenko	University of Luxembourg

Morocco

Dr. Meriem Benyahya	University Mohammed VI Polytechnic

New Zealand

Dr. Brian E. Carpenter	The University of Auckland

Norway

Dr. Tor E. Bjoerstad	mnemonic AS
Prof. Katrien De Moor	Norwegian University of Science and Technology
Prof. Tjerand Silde	Norwegian University of Science and Technology
Assoc. Prof. Michael Kirkedal Thomsen	University of Oslo, University of Copenhagen
Prof. Staal Vinterbo	Norwegian University of Science and Technology
Prof. Øyvind Ytrehus	University of Bergen
Prof. Morten Øygarden	University of Bergen

Personal capacity

Dr. Kamil Doruk Gur	Personal capacity

Portugal

Prof. Ana Aguiar	University of Porto
Prof. Manuel Barbosa	University of Porto, INESC TEC
Sofia Celi	Brave, University of Bristol
Prof. Kevin Gallagher	NOVA Schoolf of Science and Technology
Prof. Jose Legatheaux Martins	Universidade Nova de Lisboa
Prof. Carlos Serrao	Instituto Universitario de Lisboa
Prof. Mário Gaspar da Silva	Universidade de Lisboa
Prof. Joao Vilela	University of Porto

South Korea

Prof. Sang Kil Cha	KAIST

Spain

Prof. Luis Bernal-Escobedo	Universidad de Murcia
Dr. Eliseu Frígols i Brines	Universitat de València
Dr. Ignacio Cascudo	IMDEA Software Institute
Prof. Rodrigo Roman Castro	Universidad de Malaga
Prof. Josep Domingo-Ferrer	Universitat Rovira i Virgili
Prof. Jordi Domingo-Pascual	Universitat Politècnica de Catalunya
Prof. Jose Maria de Fuentes	Universidad Carlos III de Madrid
Dr. David Arroyo Guardeño	Consejo Superior de Investigaciones Científicas
Dr. Marco Guarnieri	IMDEA Software Institute
Prof. Jordi Herrera-Joancomarti	Universitat Autònoma de Barcelona
Prof. Lorena González Manzano	University Carlos III of Madrid
Prof. David Megías	Universitat Oberta de Catalunya
Dr. Pedro Moreno-Sanchez	IMDEA Software Institute
Dr. Alfonso Muñoz	Criptored
Dr. Marta Bellés Muñoz	Pompeu Fabra University
Prof. Antonio Nappa	Zimperium Inc.
Dr. Cristina Pérez-Solà	Universitat Autònoma de Barcelona
Prof. Ruben Rios	Universidad de Malaga
Prof. Jordi Castella Roca	Universitat Rovira i Virgili
Dr. Jesús García Rodríguez	Universidad de Murcia
Prof. Ricardo J. Rodríguez	Universidad de Zaragoza

Prof. Enrique Soriano-Salvador	Universidad Rey Juan Carlos
Prof. Jose Such	Consejo Superior de Investigaciones Científicas
Prof. Juan Tapiador	Universidad Carlos III de Madrid
Prof. María Isabel González Vasco	Universidad Carlos III de Madrid

Sweden

Dr. Simon Bouget	RISE Research Institutes of Sweden
Dr. Niklas Broberg	Chalmers University of Technology
Prof. Dr.-Ing. Meiko Jensen	Karlstad University
Dr. Tobias Pulls	Karlstad University
Dr. Apostolos Pyrgelis	Research Institutes of Sweden
Dr. Marco Tiloca	Research Institutes of Sweden
Prof. Björn Victor	Uppsala University

Switzerland

Prof. Matilda Backendal	Università della Svizzera italiana
Dr. Andrea Basso	IBM Research
Dr. Cecilia Boschini	ETH Zurich
Antonis Chariton	Cisco
Prof. Dr. Anastasija Collen	University of Applied Sciences and Arts of Western Switzerland
Dr. Gero Dittmann	Personal capacity
Dr. Luca De Feo	Personal capacity
Dr. Rune Fiedler	ETH Zurich
Dr. Tommaso Gagliardoni	Personal capacity

Dr. Phillip Gajland	IBM Research
Prof. Jean-Pierre Hubaux	EPFL
Dr. Lenka Marekova	ETH Zurich
Dr. Simon-Philipp Merz	ETH Zurich
Prof. Kenneth Paterson	ETH Zurich
Prof. Mathias Payer	EPFL
Prof. Kaveh Razavi	ETH Zurich
Dr. Raphael M. Reischuk	National Test Institute for Cybersecurity
Dr. Theresa Stadler	EPFL
Dr. Piet De Vaere	Product Security Guru
Dr. Jordi Weiss	Personal capacity

The Netherlands

Dr. Gunes Acar	Radboud University
Dr. Greg Alpar	Radboud University
Dr. Jacob Appelbaum	Eindhoven University of Technology
Dr. Andreas Athanasiou	TU Delft
Prof. Jeanne Mifsud Bonnici	University of Groningen
Dr. Ir. Jurjen N.E. Bos	Worldline
Dr. Andrea Continella	University of Twente
Prof. Joan Daemen	Radboud University
Assist. Prof. Alexandra Dirksen	University of Twente
Dr. Thijs van Ede	University of Twente
Dr. Thomas Fabry	European Centre on Privacy and Cybersecurity, Maastricht University

Dr. Malvin Gattinger	University of Amsterdam
Prof. Cristiano Giuffrida	VU Amsterdam
Dr. Seda Gürses	TU Delft
Dr. Florian Hahn	University of Twente
Prof. Dr. Jaap-Henk Hoepman	Radboud University, Karlstad University
Prof. Kathrin Hoevelmanns	Eindhoven University of Technology
Dr. Slinger Jansen	Utrecht University
Dr. Konrad Kollnig	Maastricht University
Dr. Matthijs Koot	University of Amsterdam
Dr. Eleftheria Makri	Leiden University
Prof. Bart Mennink	Maastricht University
Dr. Kostas Papagiannopoulos	University of Amsterdam
Dr. Paola de Perthuis	CWI
Dr. Joop van de Pol	Trail of Bits
Prof. Savio Sciancalepore	Eindhoven University of Technology
Dr. Boris Skoric	Eindhoven University of Technology
Dr. Monika Trimoska	Eindhoven University of Technology
Dr. Christine Utz	Radboud University
Dr. Jeroen van der Ham-de Vos	University of Twente
Dr. Emmanuele Zambon	Eindhoven University of Technology

Turkey

Prof. Cihangir Tezcan	Middle East Technical University

United Kingdom

Prof. Martin Albrecht	King's College London
Prof. Eerke Boiten	De Montfort University
Prof. Bill Buchanan	Edinburgh Napier University
Prof. Nathan Clarke	University of Plymouth
Dr. Simone Colombo	King's College London
Prof. Guido Noto La Diega	University of Strathclyde
Dr. Benjamin Dowling	King's College London
Prof. Tariq Elahi	University of Edinburgh
Dr. Joel Felderhoff	King's College London
Prof. Alice Hutchings	University of Cambridge
Dr. Dennis Jackson	Mozilla
Prof. Rikke Bjerg Jensen	Royal Holloway, University of London
Dr. Dan Jones	Royal Holloway, University of London
Prof. Markulf Kohlweiss	University of Edinburgh
Prof. Douwe Korff	London Metropolitan University
Prof. Andrew Martin	University of Oxford
Prof. Sarah Meiklejohn	UCL
Dr. Ngoc Khanh Nguyen	King's College London
Dr. Eamonn Postlethwaite	King's College London
Prof. Kasper Rasmussen	University of Oxford
Prof. Sophie Stalla-Bourdillon	University of Southampton, VUB
Dr. Christian Weinert	Royal Holloway, University of London
Prof. Alan Woodward	University of Surrey

United States of America

Prof. Jonathan Aldrich	Carnegie Mellon University
Brian Behlendorf	Electronic Frontier Foundation
Prof. Jon Callas	Indiana University
Prof. Ran Canetti	Boston University
Dr. Alishah Chator	Baruch College
Dr. Daniel Collins	New York University, Hebrew University
Dr. Lorrie Cranor	Carnegie Mellon University
Dr. Roger Dingledine	The Tor Project
Dr. Felix Engelmann	Ohio State University
Jeremy Epstein	Georgia Institute of Technology
Dr. Richard Forno	University of Maryland Baltimore County
Dr. Christina Garman	Purdue University
Prof. Eric Goldman	Santa Clara University
Dr. Gabriel Kaptchuk	University of Maryland
Prof. Vasileios Kemerlis	Brown University
Dr. Deepak Kumar	University of California San Diego
Prof. Susan Landau	Tufts University
Prof. Dave Levin	University of Maryland
Prof. Anna Lysyanskaya	Brown University
Prof. Michelle Mazurek	University of Maryland
Prof. Sascha Meinrath	Penn State University
Prof. Jess Miers	University of Akron
Prof. Michalis Polychronakis	Stony Brook University
Dr. Niels Provos	Security Blueprints, LLC
Dr. Elissa Redmiles	Georgetown University

Dr. Amanda Reid	University of North Carolina at Chapel Hill
Prof. Ronald L. Rivest	MIT
Adam Shostack	Shostack + Associates
Prof. Eugene H. Spafford	Purdue University
Dr. Michael A. Specter	Georgia Institute of Technology
Dr. Alin Tomescu	Aptos Labs
Prof. Eran Tromer	Boston University
Dr. Nicholas Weaver	International Computer Science Institute
Prof. Steven Weber	UC Berkeley
Dr. Tara Whalen	World Wide Web Consortium
Tarah Wheeler	TPO Group
Dr. Daniel Zappala	Brigham Young University