Any media contacts should be sent to one of

- **US Press:** James Larus: james.larus@epfl.ch
- **EU Press:** Kenny Paterson: kenny.paterson@inf.ethz.ch
- **UK Press:** Michael Veale: m.veale@ucl.ac.uk
- **RoW:** Nigel Smart: nigel.smart@kuleuven.be
- **Dutch/French** Bart Preneel: bart.preneel@esat.kuleuven.be
- **German** Cas Cremers: cremers@cispa.saarland
- **Spanish** Carmela Troncoso: carmela.troncoso@epfl.ch
- **Italian** Dario Fiore: dario.fiore@imdea.org

**Joint Statement on Contact Tracing: Date 19th April 2020**

The undersigned represent scientists and researchers from across the globe. The current COVID-19 crisis is unprecedented and we need innovative ways of coming out of the current lockdowns. However, we are concerned that some “solutions” to the crisis may, via mission creep, result in systems which would allow unprecedented surveillance of society at large.

Contact tracing is a well-understood tool to tackle epidemics, and has traditionally been done manually. However, manual contact tracing is time-consuming and is limited to people who can be identified.

In some situations, so-called “contact tracing Apps” on peoples’ smartphones may improve the effectiveness of the manual contact tracing technique. These Apps would allow the persons with whom an infected person had physical interaction to be notified, thus enabling them to go into quarantine. The Apps would work by using Bluetooth or geolocation data present in smartphones. Though the effectiveness of contact tracing Apps is controversial, we need to ensure that those implemented preserve the privacy of their users, thus safeguarding against many other issues, noting that such Apps can otherwise be repurposed to enable unwarranted discrimination and surveillance.

Research has demonstrated that solutions based on sharing geolocation (i.e., GPS) to discover contacts lack sufficient accuracy and also carry privacy risks because the GPS data is sent to a centralized location. For this reason, Bluetooth-based solutions for automated contact tracing are strongly preferred when available.

Some of the Bluetooth-based proposals respect the individual's right to privacy, whilst others would enable (via mission creep) a form of government or private sector surveillance that would catastrophically hamper trust in and acceptance of such an application by society at large. It is crucial that citizens trust the applications in order to produce sufficient uptake to make a difference in tackling the crisis. It is vital that, in coming out of the current crisis, we do not create a tool that enables large scale data collection on the population, either now or at a later time. Thus, solutions which allow reconstructing invasive information about the population should be rejected without further discussion. Such information can include the “social graph” of who someone has physically met over a period of time.
With access to the social graph, a bad actor (state, private sector, or hacker) could spy on citizens’ real-world activities. Some countries are seeking to build systems which could enable them to access and process this social graph. On the other hand, highly decentralized systems have no distinct entity that can learn anything about the social graph. In such systems, matching between users who have the disease and those who do not is performed on the non-infected users’ phones as anonymously as possible, whilst information about non-infected users is not revealed at all.

To aid the development of contact tracing without a centrally controlled database that holds private information on individuals, Google and Apple are developing infrastructure to enable the required Bluetooth operations in a privacy protective manner. Teams building the privacy protective schemes fully support this effort as it simplifies—and thus speeds up—the ability to develop such Apps. We applaud this initiative and caution against collecting private information on users. Some who seek to build centralized systems are pressuring Google and Apple to open up their systems to enable them to capture more data.

It is worth noting that the European Parliament on April 17th gave their support to the decentralized approach, pointing out by overwhelming majority "that [...] the generated data are not to be stored in centralised databases, which are prone to potential risk of abuse and loss of trust and may endanger uptake throughout the Union" and demanding “that all storage of data be decentralised”.

There are a number of proposals for contact tracing methods which respect users' privacy, many of which are being actively investigated for deployment by different countries. We urge all countries to rely only on systems that are subject to public scrutiny and that are privacy preserving by design (instead of there being an expectation that they will be managed by a trustworthy party), as a means to ensure that the citizen's data protection rights are upheld.

The following principles should be at least adopted going forward:

- Contact tracing Apps must only be used to support public health measures for the containment of COVID-19. The system must not be capable of collecting, processing, or transmitting any more data than what is necessary to achieve this purpose.
- Any considered solution must be fully transparent. The protocols and their implementations, including any sub-components provided by companies, must be available for public analysis. The processed data and if, how, where, and for how long they are stored must be documented unambiguously. Such data collected should be minimal for the given purpose.
- When multiple possible options to implement a certain component or functionality of the app exist, then the most privacy-preserving option must be chosen. Deviations from this principle are only permissible if this is necessary to achieve the purpose of the app more effectively, and must be clearly justified with sunset provisions.
- The use of contact tracing Apps and the systems that support them must be voluntary, used with the explicit consent of the user and the systems must be designed to be able to be switched off, and all data deleted, when the current crisis is over.
Signed:

Australia
Prof. Dali Kaafar    Macquarie University
Prof. Vanessa Teague    Thinking Cybersecurity and Australian National University
Dr. Yuval Yarom    The University of Adelaide and Data61

Austria
Prof. Daniel Gruss    Graz University of Technology
Prof. Stefan Mangard    Graz University of Technology
Prof. Elisabeth Oswald    University of Klagenfurt
Prof. Christian Rechberger    Graz University of Technology

Belgium
Prof. Claudia Diaz    KU Leuven
Prof. Mireille Hildebrandt    VU Brussels
Prof. Wouter Joosen    KU Leuven
Prof. Nele Mentens    KU Leuven
Prof. Bart De Moor    KU Leuven    Fellow IEEE and SIAM
Prof. Yves Moreau    KU Leuven    Fellow ISCB
Prof. Olivier Pereira    UC Louvain
Prof. Frank Piessens    KU Leuven
Prof. Bart Preneel    KU Leuven    Fellow IACR
Prof. Jean-Jacques Quisquater    UC Louvain    Fellow IACR, Member of Belgium Royal Academy
Prof. Nigel Smart    KU Leuven    Fellow IACR
Prof. François-Xavier Standaert    UC Louvain
Prof. Joos Vandewalle    KU Leuven    Fellow IEEE, IET, Eurasip, Member Royal Academy of Belgium and Academia Europaea
Prof. Ingrid Verbauwhede    KU Leuven    Fellow IEEE and Royal Academy of Belgium
Prof. Frederik Vercauteren    KU Leuven
Dr. Mathias Vermeulen    VU Brussels

Brazil
Prof. Mário S. Alvim    Universidade Federal de Minas Gerais

Canada
Prof. Vijay Ganesh    University of Waterloo
Prof. Ian Goldberg    University of Waterloo
Prof. Sergey Gorbunov    University of Waterloo
Prof. Xi He    University of Waterloo
Prof. Florian Kerschbaum    University of Waterloo
Prof. Marc-Olivier Killijian    Université du Québec à Montréal
Prof. Ali José Mashtizadeh    University of Waterloo
Prof. Alfred Menezes    University of Waterloo
Prof. Bessma Momani    University of Waterloo
Prof. Michele Mosca    University of Waterloo
Prof. Paul van Oorschot    Carleton University    Fellow ACM, IEEE and Royal Soc. Canada
Prof. Douglas Stebila    University of Waterloo
Prof. Charles Taylor    McGill University

Denmark
Prof. Ivan Damgård    Aarhus University    Fellow IACR
Prof. Claudio Orlandi    Aarhus University

Estonia
Finland
Prof. Chris Brzuska  Aalto University

France
Prof. Davide Balzarotti  EURECOM
Prof. Karide Belabas  University of Bordeaux
Dr. Olivier Blazy  University of Limoges
Dr. Jean-François Couchot  University of Franche-Comté
Prof. Aurélien Francillon  EURECOM
Prof. Nadia El Mrabet  HDR Mines Saint-Etienne
Dr. Rémis Géraud-Stewart  CentraleSupélec
Prof. Jean-Gabriel Ganascia  Sorbonne University  Fellow EURAI
Prof. Louis Goubin  University of Versailles St-Quentin-en-Yvelines
Prof. Stefan Haar  INRIA (Mexico Team)
Prof. David Kohel  Aix-Marseille University
Dr. Pascal Lafourcade  University Clermont Auvergne
Dr. Benoit Libert  ENS Lyon and CNRS
Prof. Francois Morain  LIX, Ecole Polytechnique
Prof. David Naccache  ENS Paris
Prof. Meleël Œnenn  EURECOM
Dr. Pascal Paillier  Zama
Prof. Benjamin Nguyen  INSA Centre Val de Loire
Prof. Michaël Quisquater  University of Versailles
Prof. Damien Stehlé  ENS Lyon
Prof. Jacques Stern  ENS Paris  Fellow IACR
Prof. Massimiliano Todisco  EURECOM

Germany
Prof. Michael Backes  CISPA Helmholtz Center for Information Security  Fellow IEEE
Prof. Eric Bodden  Heinz Nixdorf Institute at Paderborn University & Fraunhofer IEM
Prof. Georg Borges  Saarland University
Dr. Sven Bugiel  CISPA Helmholtz Center for Information Security
Prof. Stefan Brunthaler  Universität der Bundeswehr München
Prof. Cas Cremers  CISPA Helmholtz Center for Information Security
Dr. Jean Paul Degabriele  TU Darmstadt
Dr. Alexander Dix  European Academy for Freedom of Information and Data Protection
Prof. Christian Djeffal  TU München
Prof. Hannes Federrath  University of Hamburg  President of German Computer Society
Prof. Bernd Finkbeiner  CISPA Helmholtz Center for Information Security
Dr. Michael Friedewald  Fraunhofer ISI
Prof. Mario Fritz  CISPA Helmholtz Center for Information Security
Prof. Sascha Fahl  Leibniz University Hannover
Prof. Nils Fleischhacker  Ruhr-Universität Bochum
Prof. Dominik Herrmann  University of Bamberg
Prof. Jeanette Hofmann  Wissenschaftszentrum Berlin für Sozialforschung
Prof. Thorsten Holz  Ruhr-Universität Bochum
Prof. Albert Ingold  Johannes Gutenberg Universität Mainz
Dr. Swen Jacobs  CISPA Helmholtz Center for Information Security
Prof. Tibor Jager  University of Wuppertal
Dr. Ghassan Karame  NEC Laboratories Europe
Dr. Christian Katzenbach  Humboldt Institute for Internet and Society, Berlin
Prof. Eike Kiltz  Ruhr-Universität Bochum
Dr. Dennis-Kenji Kipker  European Academy for Freedom of Information and Data Protection
Prof. Teresa Koloma Beck  Universität der Bundeswehr München
Dr. Katharina Krombholz  CISPA Helmholtz Center for Information Security
Prof. Jörn Laml  Universität Kassel
Prof. Gregor Leander  
Ruhr-Universität Bochum

Prof. Anja Lehmann  
Hasso-Plattner-Institute and University of Potsdam

Prof. Mira Mezini  
TU Darmstadt  
Member Nat. Acad. of Engineering Sciences

Prof. Patrizia Nanz  
University of Potsdam

Prof. Paul Nolte  
Freie Universität Berlin

Prof. Christof Paar  
Max Planck Inst. CyberSec. and Privacy Fellow IACR and IEEE

Dr. Sebastian Pape  
Goethe University Frankfurt

Dr. Giancarlo Pellegrino  
CISPA Helmholtz Center for Information Security

Prof. Hartmut Pohl  
softScheck GmbH

Dr. Tina Pollmann  
TU München

Prof. Jörn Müller-Quade  
KIT Karlsruhe

Prof. Kai Rannenberg  
Goethe University Frankfurt  
Vice President IFIP

Prof. Steffen Reith  
RheinMain University of Applied Sciences

Prof. Elisa Resconi  
TU München

Prof. Alexander Roßnagel  
University of Kassel

Prof. M Angela Sasse  
Ruhr Universität Bochum

Prof. Ina Schiering  
Ostfalia University of Applied Sciences

Prof. Sebastian Schinzel  
Münster University of Applied Sciences

Prof. Stefan Schöner  
TU München

Prof. Jörg Schwenk  
Ruhr University Bochum

Prof. Juraj Somorovsky  
Paderborn University

Prof. Christoph Sorge  
Universität des Saarlandes

Dr. Ben Stock  
CISPA Helmholtz Center for Information Security

Prof. Thorsten Struwe  
KIT Karlsruhe and CeTI TU Dresden

Dr. Nils Ole Tippenhauer  
CISPA Helmholtz Center for Information Security

Prof. Jilles Vreeken  
CISPA Helmholtz Center for Information Security

Prof. Andreas Zeller  
CISPA Helmholtz Center for Information Security  
Fellow ACM

India

Prof. Subhamoy Maitra  
Indian Statistical Institute

Dr. Mridul Nandi  
Indian Statistical Institute

Prof. Manoj Prabhakaran  
IIT Bombay

Dr. Somitra Kr. Sanadhya  
IIT Ropar

Prof. Sandeep Kumar Shukla  
IIT Kanpur  
Fellow IEEE

Italy

Prof. Rainer Bauböck  
European University Institute, Florence

Prof. Carlo Blundo  
Università di Salerno

Prof. Dario Catalano  
Università di Catania

Prof. Ciro Cattuto  
University of Turin

Prof. Giovanni Comandè  
Scuola Superiore Sant'Anna, Pisa

Prof. Mauro Conti  
Università di Padova

Prof. Giuseppe Persiano  
Università di Salerno

Prof. Daniele Venturi  
Sapienza University of Rome

Prof. Ivan Visconti  
University of Salerno

Israel

Prof. Katya Assaf  
Hebrew University

Prof. Yehuda Lindell  
Bar-Ilan University

Prof. Benny Pinkas  
Bar-Ilan University

Japan

Prof. Tetsu Iwata  
Nagoya University

Prof. Kazuo Sakiyama  
UEC Tokyo

Luxembourg

Prof. Peter Y A Ryan  
University of Luxembourg
Portugal
Dr. Manuel Barbosa University of Porto (FCUP) and INESC TEC

Mexico
Dr. Cuauhtemoc Mancillas-López CINVESTAV-IPN
Dr. Brisbane Ovilla-Martínez CINVESTAV-IPN
Dr. Francisco Rodríguez-Henríquez CINVESTAV-IPN

The Netherlands
Prof. Lejla Batina Radboud University
Prof. Peter Boncz CWI Amsterdam and VU University Amsterdam
Prof. Jos Baeten CWI Amsterdam and University of Amsterdam
Prof. Ronald Cramer CWI Amsterdam and Leiden University Fellow IACR
Prof. Joan Daemen Radboud University
Prof. Arie van Deursen TU Delft
Prof. Aaron Ding TU Delft
Dr. Leo Ducas CWI Amsterdam
Prof. Michel van Eeten TU Delft
Prof. Serge Fehr CWI Amsterdam and Leiden University
Prof. Tobias Fiebig TU Delft
Prof. Natali Helberger University of Amsterdam
Prof. Lisa Herzog University of Groningen
Prof. Marijn Janssen TU Delft
Prof. Tanja Lange Eindhoven University of Technology
Prof. Arno R. Lodder Vrije Universiteit Amsterdam
Prof. Veelasha Moonsamy Radboud University
Prof. Stefanie Roos TU Delft
Prof. Peter Schwabe Radboud University
Dr. Benne de Weger Eindhoven University of Technology
Dr. Philip Zimmermann TU Delft

New Zealand
Prof. Steven Galbraith University of Auckland

Norway
Prof. Kristian Gjøsteen NTNU

Slovenia
Prof. Marko Holbl University of Maribor

Spain
Prof. Manuel Carro IMDEA Software Institute and Technical University of Madrid
Prof. Ignacio Cascudo IMDEA Software Institute
Gemma Galdon Clavell Etics Foundation
Prof. Dario Fiore IMDEA Software Institute
Prof. Ramon Lopez de Mantaras Artificial Intelligence Research Institute Fellow of EurAI
Prof. Juan Tapiador UC3M
Prof. Narseo Vallina-Rodriguez IMDEA Networks Institute
Prof. María Isabel González Vasco Universidad Rey Juan Carlos

Sweden
Prof. Rose-Mhari Ahlfeldt University of Skövde
Dr. Matthias Beckerle Karlstad University
Prof. Simone Fischer-Hübner Karlstad University
Dr. Leonardo Martucci Karlstad University
Mr. Linus Nordberg DFRI
Dr. Tobias Pulls Karlstad University
Switzerland
Prof. David Basin ETH Zurich Fellow ACM
Dr. Peter Berlich ZHAW
Dr. Jan Beutel ETH Zurich
Prof. Edouard Bugnion EPFL Fellow ACM
Prof. Christian Cachin University of Bern Fellow ACM and IEEE
Prof. Srdjan Čapkun ETH Zurich Fellow ACM
Prof. Bryan Ford EPFL
Prof. Dennis Hofheinz ETH Zurich Fellow ACM and IEEE
Prof. Jean-Pierre Hubaux EPFL
Prof. James Larus EPFL Fellow ACM
Prof. Ueli Maurer ETH Zurich Fellow ACM, IACR and IEEE
Prof. Adrian Perrig ETH Zurich Fellow ACM
Prof. Kenny Paterson ETH Zurich Fellow IACR
Prof. Mathias Payer EPFL
Prof. Kaveh Razavi ETH Zurich
Prof. Marcel Salathé EPFL
Prof. Carmela Troncoso EPFL

United Arab Emirates
Prof. Christina Pöpper New York University, Abu Dhabi.

United Kingdom
Prof. Martin Albrecht Royal Holloway, University of London
Dr. Reuben Binns University of Oxford
Prof. Lorenzo Cavallaro King's College London
Prof. Liquin Chen University of Surrey
Prof. Carlos Cid Royal Holloway, University of London
Dr. Jennifer Cobbe University of Cambridge
Prof. Jon Crowcroft University of Cambridge FRS, FREng Fellow ACM and IEEE
Prof. George Danezis UCL
Prof. Lilian Edwards Newcastle University
Prof. Flavio Garcia University of Birmingham
Dr. Robert Granger University of Surrey
Dr. Jassim Happa Royal Holloway, University of London.
Dr. Rikke Bjerg Jensen Royal Holloway, University of London
Dr. Philipp Jovanovic UCL
Prof. Aggelos Kiayias University of Edinburgh
Prof. Christopher Marsden University of Sussex
Prof. Keith Martin Royal Holloway, University of London
Prof. Ivan Martinovic University of Oxford
Dr. Tim Muller University of Nottingham
Dr. Dan Page University of Bristol
Dr. Elizabeth Quaglia Royal Holloway, University of London
Prof. Mark D. Ryan University of Birmingham
Prof. Burkhard Schaefer University of Edinburgh
Prof. Steve Schneider University of Surrey Fellow IET
Dr. Jat Singh University of Cambridge
Prof. Max Van Kleek University of Oxford
Dr. Michael Veale UCL
Prof. Alan Woodward University of Surrey Fellow BCS and InstP
Dr. Vassiles Zikas University of Edinburgh

United States of America
Prof. Alessandro Acquisti Carnegie Mellon University
Dr. Johanna Amann ICSI
Prof. Adam Bates Uni. of Illinois at Urbana-Champaign
Appendix:

Privacy-preserving decentralized methods of the type referred to in this document include:

- **DP-3T**: [https://github.com/DP-3T](https://github.com/DP-3T)
- **TCN Coalition**: [https://tcn-coalition.org/](https://tcn-coalition.org/)
- **PACT (MIT)**: [https://pact.mit.edu/](https://pact.mit.edu/)
- **PACT (UW)**: [https://covidsafe.cs.washington.edu/](https://covidsafe.cs.washington.edu/)

All these teams are committed to working together to make their systems interoperable. They aim to provide different decentralized privacy preserving methods which can be adapted by countries depending on their local situation. By working together they can ensure that using contact tracing in the effort to defeat COVID-19 can be done in a way that protects privacy.