Response to Australia's Defence Trade Controls Act

July 6, 2015

We are deeply concerned about Australia's Defence Trade Controls Act (DTCA). The act prohibits the "intangible supply" of encryption technologies, and hence subjects many ordinary teaching and research activities to unclear, potentially severe, export controls. As an international organization of cryptographic researchers and educators, we are concerned that the DTCA criminalizes the very essence of our association: to advance the theory and practice of cryptography in the service of public welfare.

We affirm that the public welfare of Australians — and society in general — is best served by open research and education in cryptography and cybersecurity. Open, international scientific collaboration is responsible for the encryption technologies that are now vital to individuals, businesses, and world governments alike. The current legislation cuts off Australia from the international cryptographic research community and jeopardizes the supply of qualified workforce in Australia's growing cybersecurity sector.

We call on Australia to amend their export control laws to include clear exemptions for scientific research and for education.

IACR Member Signatories (187): add your signature!

- Christian Cachin, President of the IACR, IBM Research - Zurich, Switzerland
- Nigel Smart, Vice President IACR, University of Bristol, United Kingdom
- Gregory Rose, Cryptography Consultant, Australian citizen and IACR treasurer, United States
- Michel Abdalla, Director of the IACR, École Normale Supérieure & CNRS, France
- David Pointcheval, Senior Researcher, Director of the IACR, École Normale Supérieure & CNRS, Franc
- Moti Yung, IACR Board Member, USA
- Mike Rosulek, IACR Communications Secretary & Assistant Professor, Oregon State University, USA
- Bart Preneel, IACR Board Member, Full Professor, KU Leuven, Belgium
- Thomas A. Berson, Director of IACR, Anagram Laboratories, United States
- Yuval Yarom, The University of Adelaide, Australia
- Douglas Stebila, Queensland University of Technology, Australia
- Josef Pieprzyk, Queensland University of Technology, Australia
- Vanessa Teague, University of Melbourne, Australia
- Doche Christophe, Macquarie University, Australia
- Ron Steinfeld, Monash University, Australia
- Benjamin Dowling, Queensland University of Technology, Australia
- Yehuda Lindell, Professor, Bar-Ilan University, Israel
- Duong-Hieu Phan, Assistant Professor, University of Paris 8, France
- Ivan Damgard, Aarhus University, Denmark
- Martijn Stam, University of Bristol, United Kingdom
- Steven Galbraith, University of Auckland, New Zealand
- Sherman S.M. Chow, Chinese University of Hong Kong (CUHK), Hong Kong
- Stefan Dziembowski, University of Warsaw, Poland
- Jean Paul Degabriele, Royal Holloway, United Kingdom
- Vanishree Rao, UCLA, United States
- Phillip Rogaway, University of California, Davis, United States
- Emmanuela Orsini, University of Bristol, United Kingdom
- Tiago Fonseca, Gama Faculty - University of Brasilia, Brazil
- Silas Richelson, UCLA, United States
- Damien Stehlé, ENS de Lyon, France
- Thomas Peyrin, Nanyang Technological University, Singapore
- Moises Salinas-Rosales, Faculty at IPN Computing Research Center (CIC) MX, Mexico
- Nadia Heninger, University of Pennsylvania, United States
- Olivier Blazy, Université de Limoges, France
- Craig Costello, Microsoft Research, United States
- Paulo Barreto, University of São Paulo, Brazil
- Patrick Derbez, SnT, University of Luxembourg, Luxembourg
- Stephen Lombardo, Zetetic LLC, United States
- Alejandro Hevia, University of Chile, Chile
- Dario Fiore, IMDEA Software Institute, Madrid, Spain
- Michael J. Markowitz, Information Security Corp., United States
- Robert Amzi Jeffs, Harvey Mudd College, United States
- Abhishek Banerjee, Georgia Institue of Technology, United States
- Yuliang Zheng, University of Alabama at Birmingham, United States
- Mike Hamburg, United States
- Manoj Prabhakaran, Associate Professor, University of Illinois at Urbana-Champaign, United States
- Deepesh Data, Tata Institute of Fundamental Research, Mumbai, India
- Steven Myers, Associate Professor, Indiana University, United States
- Benedikt Gierlichs, KU Leuven, Belgium
- Mridul Nandi, Indian Statistical Institute, Kolkata, India
- Saqib A. Kakvi, University of Bristol, United Kingdom
- Gaëtan LEURENT, INRIA, France
- Leo Ducas, CWI, The Netherlands
- Stefan Mangard, Professor, Graz University of Technology, Austria
- Razvan Barbulescu, CNRS, France
- Alexandre Anzala Yamajako, Thales Communication & Security, France
- Serge Fehr, CWI Amsterdam, The Netherlands
- Fabrice Benhamouda, Ecole Normale Supérieure, France
- Eduardo Soria Vázquez, Spain
- Pablo Rauzy, Telecom ParisTech, France
- Florian Mendel, Senior Researcher, Graz University of Technology, Austria
- Léo Perrin, SnT, University of Luxembourg, Luxembourg
- Olivier Billet, IACR Member, France
- Richard OUTERBRIDGE, Canada
- Tobias Boelter, UC Berkeley, USA

- Maria Eichlseder, Graz University of Technology, Austria
- Reza Ebrahimi Atani, University of Guilan, Iran
- Khoa Nguyen, Nanyang Technological University, Singapore
- Ignacio Cascudo, Aarhus University, Denmark
- Randy Bush, IIJ Research Laboratory & Dragon Research Labs
- Martin Albrecht, Information Security Group, Royal Holloway, University of London, United Kingdom
- Andreas Aßmuth, Ostbayerische Technische Hochschule (OTH) Amberg-Weiden, Germany
- Jean-Bernard Fischer, NagraVision, Switzerland
- Stig F. MJOLSNES, Norwegian University of Science & Technology, Norway
- Ron RIVEST, MIT, United States
- Dominique Unruh, Professor of Information Security, University of Tartu, Estonia
- Aaron Zauner, lambda.co.at, Austria
- Andrew Clark, Primary Key Associates Limited, United Kingdom
- Karim ElDefrawy, United States
- Somindu Ramanna, ENS Lyon, France
- Eran Tromer, Tel Aviv University, Israel
- Bogdan Warinschi, University of Bristol, United Kingdom
- Qiong Huang, South China Agricultural University, China
- Felix Günther, Technische Universität Darmstadt, Germany
- Pierre Karpman, Inria / X-NTU, France
- Tal Moran, IDC Herzliya, Israel
- Atsushi FUJIOKA, Kanagawa University, Japan
- Jens Groth, University College London, United Kingdom
- Paul Grubbs, Skyhigh Networks, United States
- Daniele Micciancio, professor, UCSD, United States
- Alessandra Scafuro, BU and NEU, United States
- Seokhie Hong, CIST, Republic of Korea
- Yuriy Aydarov, Perm State University, Russian Federation
- Shai Halevi, IBM Research, United States
- Naofumi Homma, Tohoku U, Japan
- Sahadeo Padhye, Department of Mathematics, MNNIT Allahabad (India), India
- Palash Sarkar, Professor, Indian Statistical Institute, India
- Jonathan Katz, University of Maryland, United States
- Huseyin Demirci, TUBITAK BILGEM, Turkey
- Jian Guo, Nanyang Technological University, Singapore
- Christina Boura, Université de Versailles, France
- Tancrède Lepoint, France
- Colin BOYD, Norwegian University of Science and Technology (NTNU), Norway
- Peter Schwabe, Radboud University, The Netherlands
- Victoria Fehr, TU Darmstadt, Germany
- Stefan Katzenbeisser, Professor, Technische Universitaet Darmstadt, Germany
- Thomas Martin, Khalifa University, United Arab Emirates
- Tore Frederiksen, Aarhus University, Denmark
- Håvard Raddum, Simula Research Laboratory, Norway
- Willi Meier, FHNW , Switzerland
- Serge Vaudenay, Professor, EPFL, Switzerland
- Benjamin Smith, INRIA / École polytechnique, France
- Daniele Venturi, Sapienza University of Rome, Italy
- Tanja Lange, Technische Universiteit Eindhoven, The Netherlands
- Alexandre Duc, EPFL, Switzerland
- Frederic Jouret, France
- Stefan Kölbl, Technical University of Denmark, Denmark
- Grigory Karpunin, Lomonosov Moscow State University, Russian Federation
- Carla Ràfols, Ruhr-Universität Bochum, Germany
- Philip Ittmann, University of Cape Town, South Africa
- Christine Swart, University of Cape Town, South Africa
- Victor Lomne, France
- Mario Lamberger, Senior Cryptographer, NXP Semiconductors, Austria
- Serge Gautier, Cartes Bancaires, France
- Britta Hale, Research Fellow, NTNU, Norway
- Christoph Bader, Ruhr University Bochum, Germany
- Roberto Trifiletti, Aarhus University, Denmark
- Sonia Bogos, EPFL, Switzerland
- Jeroen Doumen, The Netherlands
- István Lám, Tresorit, Hungary
- Robert R. Enderlein, IBM Research Zurich & ETH Zurich, Switzerland
- Ruben Niederhagen, Eindhoven University of Technology, The Netherlands
- Christian Rechberger, DTU , Denmark
- Tim Güneysu, Ruhr-Universität Bochum, Germany
- Benoit Libert, ENS de Lyon, France
- Christian Janson, Information Security Group, Royal Holloway, University of London, United Kingdom
- Brecht Wyseur, NAGRA, Switzerland
- Afonso Arriaga, University of Luxembourg, Luxembourg
- Niv Gilboa, Ben-Gurion University, Israel
- Weijun Shan, Shanghai Fudan Microelectronics Group Co., Ltd., China
- Tyge Tiessen, Technical University of Denmark, Denmark
- Maximilian Fillinger, CWI, The Netherlands
- Neil Hanley, Queens University Belfast, United Kingdom
- Tal Malkin, Columbia University, United States
- Orr Dunkelman, University of Haifa, Israel
- Bernardo Machado David, Aarhus University, Denmark
- Sunoo Park, MIT, United States
- Damien Vergnaud, Ecole normale superieure, France
- Anne CANTEAUT, INRIA , France
- Stephan Krenn, AIT Austrian Institute of Technology GmbH, Austria
- Damian Vizár, EPFL, Switzerland
- Sanjay Bhattacherjee, ENS-Lyon, France
- Wanja Vogel, Germany
- Mikhail Ponomarev, Russian Federation
- Joppe W. Bos, Cryptographer, NXP Semiconductors, Belgium
- Juan A. Garay, Yahoo Labs, United States
- Kai-Min Chung, Academia Sinica, Taiwan, ROC
- Jesse Stern, University of Rochester, United States
- Bryan Parno, Microsoft Research, United States
- Jérémy JEAN, Nanyang Technological University, Singapore
- Jin Hong, Seoul National University, Republic of Korea

- Peter Scholl, University of Bristol, United Kingdom
- Carlos Cid, Royal Holloway, University of London, United Kingdom
- Filip Zagorski, Wroclaw University of Technology, Poland
- Yu Yu, IACR webmaster, Shanghai Jiao Tong University, China
- Joost Rijneveld, Radboud University, The Netherlands
- Hua Wu, The George Washington University, China
- Helena Handschuh, Cryptography Research, United States
- Carl Ellison, Ellison Consulting LLC, United States
- Mikkel Krøigaard, Denmark
- Shoichi Hirose, University of Fukui, Japan
- Sylvain Pelissier, Switzerland
- Pascale Charpin, INRIA - Paris-Rocquencourt, France
- Michael Tunstall, Cryptography Research, United States
- Benny Applebaum, Tel Aviv University, Israel
- MAHARDIKA SOFFAN PUTRA, NATIONAL CRYPTO AGENCY OF REPUBLIC OF INDONESIA, Indonesia
- Tommaso Gagliardoni, TU Darmstadt, Germany
- Martin M. Lauridsen, DTU, Denmark
- Jean-Luc Beuchat, Switzerland
- Bart Mennink, KU Leuven, Belgium
- Minhye Seo, Korea University, Republic of Korea
- Kwangsu Lee, Korea University, Republic of Korea
- Philipp Jovanovic, University of Passau, Germany
- Giorgia Azzurra Marson, TU Darmstadt, Germany
- Alexander Dent, United Kingdom
- Tatsuaki OKAMOTO, NTT, Japan
- Reza Reyhanitabar, École Polytechnique Fédérale de Lausanne, Switzerland

Other Endorsements

The following organizations have also endorsed the petition:

- Australian Privacy Foundation
- Electronic Frontier Foundation
- Privacy & Access Council of Canada

Media

- The Register: 'Save the teachers!' 184 cryptologists send Oz Govt cleartext petition
- IT News: Experts protest Aussie law banning crypto export

About the IACR

The International Association for Cryptologic Research (IACR) is a non-profit scientific organization whose purpose is to further research in cryptology and related fields. Cryptology is the science and practice of designing computation and communication systems which are secure in the presence of adversaries.

Direct feedback about this petition to petitions@iacr.org .

Copyright © 2015 IACR