

# Cryptographers' statement on Australian export controls on cryptography research

*Supplementary Submission to the inquiry into the implementation of the defence trade controls legislation*

Submitted by Vanessa Teague, [viteague@unimelb.edu.au](mailto:viteague@unimelb.edu.au) , June 2015

Senator Chris Back

Chair Foreign Affairs, Defence and Trade Legislation Committee

Dear Senator Back,

I am currently attending an extended cryptography research meeting at UC Berkeley. In the attached statement, many of the attendees have expressed their deep concern over Australian export control restrictions applied to cryptography research. The signatories to this statement include some of the finest cryptographers in the world, inventors of the algorithms we rely on every day for electronic security and privacy. It is a tremendous privilege for me to be able to work with these people. This is exactly the sort of free exchange of new ideas that Australians will be excluded from under the DTCA unless there is an exemption for scientific research.

Yours Sincerely,

A handwritten signature in black ink, appearing to read 'V. Teague'.




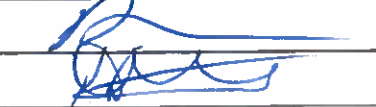






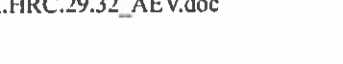

Vanessa Teague.

## Cryptographers' statement on Australian export controls on cryptography research








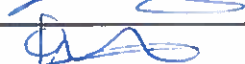













We are deeply concerned about Australia's defence export controls restricting cryptographic research.

The academic freedom provided to cryptography researchers in Israel, the US, and most of Europe, is paramount to building a strong research community in cryptography and cyber-security. Australian researchers need to participate freely in this community, or risk being left behind or discouraged from doing cryptography research at all. Local research in cryptography and computer security has great benefits to society. Researchers train Australian students to work in cyber-security, and contribute to a knowledge base that informs public debate on issues related to electronic security and privacy. Cryptography can also support political freedoms: the UN Human Rights Council's recent report on the promotion and protection of the right to freedom of opinion and expression<sup>1</sup> concluded that, "encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection."

We hope that Australia's export control laws will be amended to include an exception for scientific research, and unequivocally believe that this is in the best interests of Australian society.

Name	Affiliation	Signature
PROF. YEHUDA LINDELL	BAR-ILAN UNIV. ISRAEL	
VANESSA TEAGUE	UNIVERSITY OF MELBOURNE	V. Teague
Huijia Lin	UCSB	
Maricela Raykova	SRI	
Aloni Cohen	MIT	
AMIT SAHAI	UCLA	
Yury Dodos	NYU	
CLAUDIO ORLANDI	AARHUS UNIVERSITY, DK	
Abhishek Jain	JHU	
Ivan Damgård	Aarhus University	
Yuhai Ishai	Technion	
Elette Boyle	Technion Israel	
MOTI YUDG	JACK BOARD MEMBER	

<sup>1</sup> [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32\\_AEV.doc](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc)

Adam B. Well	Georgetown	
KARIM ELDEFRAWY	HRL LABORATORIES	
PRATIHA MUKHERJEE	AARHUS UNIV.	
MIYAKO OHKUBO	NICT	大久保 美子
Ryo Nishimaki	NTT	Ryo Nishimaki
Saleet Klein	Tel Aviv University	· sigbo
Ron Rothblum	Weizmann Institute	Ron Rothblum
Mehdi Tibouchi	NTT	
Alain Passelègue	ENS	
Tianren Liu	MIT	Tianren
C. PANDU RANGAN	IITM, INDIA	
Kane YANG	U of Waterloo	
Fang Song	UW	
Foteini Baldimtsi	Boston University	
Björn Tackmann	UC San Diego	Tackmann
Sunoo Park	MIT	
Ameer Mohammed	University of Virginia	
<del>XXXXXXXXXX</del>	<del>XXXX</del>	<del>XXXXXXXXXX</del>
Masayuki ABE	NTT	
RANJIT KUMAR SARKAR	MIT	
Tancrède Lepoint	cryptoExperts	
ROSARIO GENARO	CUNY, USA	
AGGELOS KIAMIAS	U. OF ATHENS, GR	
Charalampos Papamanthakis	U. Maryland	
Narcel Keller	U of Bristol	
Ron Rivest	MIT	Ron Rivest
Manuel Sabin	UC Berkeley	
Steve Myers	Indiana University	
abhi shelat	U. of VIRGINIA	

Rishabh Goyal	UT Austin	Rishabh
Prof. Tal Malkin	Columbia University	Tal Malkin
Prabhanjan Ananth	UCLA	Prabhanjan
Alon Rosen	IDC Herzliya	Alon
Vassilis Zikas	ETH Zurich	Vassilis
Michael ABDALLA	ENS Paris	Michael Abdalla
HUGO KRAWCZYK	IBM Research	Hugo Krawczyk
Michael Walfish	NYU	Michael Walfish
Samuel Zohar	UVA	Samuel Zohar
Soheil Nematihaji	UVA	Soheil Nematihaji
MIKE ROSULEK	Oregon State Univ	Mike Rosulek
MARSHALL BALL	Columbia University	Marshall Ball