Cryptography research and the Defence Export Controls Act

May 29th, 2018

This submission addresses the unintended consequences of the Defence Trade Controls Act for Australian cryptography research.

The Defence Trade Controls Act (DTCA) is Australia's implementation of the Wassenaar Arrangement, an international weapons non-proliferation agreement. Cryptography is the mathematical science of controlling the flow of information. It is not a weapon and cannot be used as a weapon. It does not belong in the Wassenaar arrangement and should be removed. Unfortunately, the arrangement does not allow Australia simply to remove parts of the treaty from our Defence Strategic Goods List.

Encryption is one of the foundations of cybersecurity. Australia's shortage of skills in this area has already been described as a threat to our future national security. Australian businesses are also clamouring for graduates with these skills as the need for in-house cybersecurity expertise becomes crucial: e.g. Banks, telcos, and the public sector. Restrictions on research and teaching of fundamental skills and new advances in cybersecurity constrict the pipeline for such graduates. This makes us less secure and makes our industries vulnerable to malicious online actors. Many Australian cryptographers work overseas, and most Australian universities struggle to find people with adequate technical cybersecurity skills. The DTCA's penalties and restrictions on the communication of cryptography research indirectly jeopardise our future national security.

It is not true that the DTCA's restrictions on communication about cryptography bring us into line with like-minded countries. Most other Wassenaar participants are liberal democracies with explicit constitutional protections of free speech. Though some have restrictions on the books, there is substantial precedent for regarding them as inconsistent with the constitutional protection of free communication. For example, in the US case of Bernstein vs the Department of Justice, the US 9th circuit court of appeal found that the export of source code for encryption was protected by the First Amendment.[1] EU directives have also emphasised the importance of encryption for protecting the right to free communication. Australia was particularly singled out by the International Association for Cryptologic Research[2] for subjecting "many ordinary teaching and research activities to unclear, potentially severe, export controls."

Australia has the challenge of implementing our obligations under the Wassenaar arrangement, knowing that some parts of it are badly in need of rewriting or removal. This is a political challenge, particularly since improving Australia's cybersecurity is a key government priority. Restricting cybersecurity research is profoundly counterproductive. (Restricting the export of secure software for commercial purposes is highly counterproductive too, but is not the subject of this submission.)

The DTCA exempts "basic research" and publication, but should be broadened to exempt "fundamental scientific research" as well. Fundamental research is *"basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community."*[3] The DTCA exempts free publication, which is good, but there is still a problem for researchers when communicating internationally, but before publication. Conducting this communication freely, spontaneously, and often, is a critical component of cryptography research. This communication often includes shared work on cryptographic algorithms and code, which are intended to be made public but are not public during initial development. Useful cryptography research is generally directed towards a specific practical objective - that's why it's useful. Most Australian cryptography research hence doesn't qualify for the "basic research" exemption as defined by DEC. A "fundamental research" exemption would protect all mathematical and scientific research that was intended to be shared broadly in the normal way of scientific work. This would protect almost all work done by university-based Australian cryptography researchers and have negligible impact on criminal behaviour.

---

1 https://caselaw.findlaw.com/us-9th-circuit/1317290.html

2 https://www.iacr.org/petitions/australia-dtca/

3 This definition is from the US Defense Advanced Research Projects Agency (DARPA) http://www.darpa.mil/work-with-us/for-universities/fundamental-research

---

Recommendation 1: Amend the DTCA to exempt “fundamental research” rather than “basic research.”

Some of us were included on the ICT working group established by the strengthened export controls steering group, which included Defence Export Controls (DEC), who have been as accommodating and flexible as they can be in the circumstances. We’ve worked together on drafting a significantly lighter and broader permit process, which will allow academics a broad permit for international cryptography research, with a requirement to notify DEC but without the need to get permission before commencing work. We’d like to thank DEC for hosting the discussion and working together on better rules. An overview of the trial is described here: http://www.defence.gov.au/ExportControls/CryptoPermitTrial.asp

In the absence of legislative change (as in Recommendation 1), the broader permits are a reasonable amelioration, though they still leave cryptography researchers at risk if there is a change of policy.

Recommendation 2: (If Recommendation 1 fails) Retain the newly-developed trial permits for general cryptography research and collaboration.

In summary,

- cryptography should be removed from the Wassenaar arrangement,
- fundamental scientific research should be exempted from the Defence Trade Controls Act,

but in the meantime the broader permits from DEC are a significant amelioration.

We would be happy to discuss any of these matters with the Inquiry.

Yours Sincerely,

Dr Vanessa Teague
Chair, Cybersecurity and Democracy Network
Melbourne School of Engineering
The University of Melbourne, Victoria 3010 Australia
Tel: +61 3 8344 1274
Email: vjteague@unimelb.edu.au

with

Professor Lynn Margaret Batten, PhD
Fellow of the Australian Computer Society
ISC2 Leadership Award in Information Security
Senior Member of the Institute of Electrical and Electronics Engineers
Deakin Research Chair in Mathematics
School of Information Technology
Deakin University, 221 Burwood Highway
VIC 3125, Australia
Office tel.: +61 3 92517474
Email: lynn.batten@deakin.edu.au
Website: www.deakin.edu.au/~lmbatten

A/Prof Xavier Boyen
ARC Future Fellow
Associate Professor, Information Security
Queensland University of Technology
Brisbane QLD 4000, Australia
Tel: +61 7 3138 2587
Email: xavier.boyen@qut.edu.au

Prof Rajeev Gore
Professor, Logic and Computation Group,
Research School of Computer Science
ANU College of Engineering and Computer Science
The Australian National University
Canberra ACT 2601
Tel: +61-2-61 25 86 03
Email: Rajeev.Gore@anu.edu.au

Dr Toby Murray, DPhil (University of Oxford)
Lecturer, School of Computing and Information Systems
University of Melbourne
http://people.eng.unimelb.edu.au/tobym/
toby.murray@unimelb.edu.au

Dr Josef Pieprzyk
Data 61, CSIRO

Dr. Ron Steinfeld
Senior Lecturer,
Cybersecurity Lab,
Faculty of Information Technology,
Monash University,
Clayton VIC 3800
Australia
Email: ron.steinfeld@monash.edu
Phone: +61 3 99055225

Dr Yuval Yarom
School of Computer Science
The University of Adelaide
Adelaide, SA 5005
tel: 08 8313 4727
Email: yval@cs.adelaide.edu.au