

## My response to a message by Dorothy Denning in 1995 – Australia and Encryption Policy

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-01/0341.html>

---

*From:* General X (*at11xbxb\_at\_asean-mail.com*)

*Date:* 01/05/04

Date: 5 Jan 2004 02:19:12 -0800

Dear Dorothy,

It is funny that when I lived in an automobile from 2000 to 2002 in the U.S.A. after my divorce from my former U.S. spouse I stayed on these campuses (I know that Madeleine Albright likes to stay on the university campuses – I have learned from all) where these people are actually still working. I was just a nobody and you would have ingored me as a nobody. I went to libraries etc. I was somebody who smelled occasionally and lived a very low life in the same way as Ted Kasinzky (the brilliant mathematician and unabomber) and John Nash (the Nobel Prize winner) (both are my heroes). I liked also the computer systems of Georgetown that I used without any permit although I had no access codes and rights to the system. Somebody had just left their session open. Often happens in the real world that somebody just lefts their system and session open and you do not need any codebreakers to penetrate to very critical systems (sometimes you just jump over the fence and go to the terminal). This was just before I spent my night near the White House in my automobile. Actually, I have the same automobile here in Varkaus, Finland.

Make Von Islander (X)

Also known in the city of Varkaus as a person who has still one of the surviving KGB mindsets in Varkaus.

----- Forwarded message -----

Date: Wed, 23 Aug 1995 15:29:17 -0400 (EDT)

From: Dorothy Denning <denning@cs.cosc.georgetown.edu>

To: MFROOMKI@umiami.ir.miami.edu

Cc: denning@cs.cosc.georgetown.edu

Subject: Australia and Encryption Policy

>>From denning Wed Aug 23 15:14:25 1995

Date: Wed, 23 Aug 95 15:13:05 EDT

From: denning (Dorothy Denning)

Full-Name: Dorothy Denning

sci.crypt: My response to a message by Dorothy Denning in 1995 – Australia and Encryption Policy

To: farber@cis.upenn.edu, risks@csl.sri.com, banisar@washofc.epic.org  
Subject: Australia and Encryption Policy  
Cc: denning, Ross.Anderson@cl.cam.ac.uk  
Content-Length: 4390

Ross Anderson posted a message on the net recently stating that Australia was proposing an encryption policy that would force residents to use weak cryptography while banks would get key escrow. His source was a talk by Steve Orłowski, who is Assistant Director, Security Management, in the Australian Attorney-General's Department.

Attached is a copy of an open letter by Mr. Orłowski in response to that post. He is not proposing that individuals be forced to use weak encryption. Key escrow would be an option available to anyone wanting a high level of encryption. Organizations and individuals could escrow their own keys if desired.

This message and his letter may be forwarded.

Dorothy Denning  
-----

Dear

Thank you for your comments on the subject of the use of encryption by private individuals.

Firstly I would like to make the point that the debate has arisen from one person's interpretation of a paper I gave at a conference on "Cryptography Policies and Algorithms" The full text of that paper is now available on the net at

<http://commerce.anu.edu.au/comm/staff/RogerC/RogersHome.html>

The paper carries a disclaimer at the top that the views are mine and do not necessarily represent the views of the Australian Government. The paper sets out the Government's policy on telecommunications interception, which includes the issue of the use of cryptography as: "As a result of the Report, Australia is, among other TI issues, monitoring the impact of encryption in the telecommunications interception area and will re-examine matters in 1997 following the opening of the telecommunications area to full competition." Telecommunications covers both voice and data communications.

The last paragraph of the paper says that there is a need to expand the cryptography debate to cover the needs of individual users in the context of the information superhighway rather than current Internet users. The paper also points out that issues such as cost, convenience

and public confidence in cryptography systems will be the main issues. Public confidence is explained in terms that as long as it meets the general requirement for privacy it will be acceptable. I still maintain that the general user of the superhighway in the next century will be satisfied with a lower level of encryption which will meet that and cost and user friendliness requirements.

On specific point made in the Internet message, the paper does not suggest, either directly or by implication, that individuals should be banned from using encryption.

Regarding the use of higher level encryption, the paper supports the concept of commercial key escrow where organisations hold their own keys but may be required to provide them in response to a court order. The same would apply to individuals who could either hold their own keys or store them with a commercial body. Access to those keys would be by court order and in that respect is no different to existing procedures for the interception or seizure of telephone conversations or paper records. There is no suggestion that these basic principles, and protection of individual's rights in general, should be changed

If individuals were to use lower level encryption there would be no need for them to maintain copies of any keys for such systems. To my mind this is preferable to a requirement for keys to be maintained for all encryption systems, which could be the result if universal key escrow were introduced.

Finally on the question of interception, the general public expects a reasonable level of law enforcement to ensure the protection of their person and property. Governments are required to find a balance between this and the rights of individuals to privacy. Part of this balance is to ensure that law enforcement authorities convince a court that there is a need to carry out an interception. There is no suggestion that this fundamental approach should be changed. The paper certainly does not suggest that the Attorney-General's Department should become a centralised interception authority. In fact such a role would not be consistent with its role as a source of advice to Government.

I hope the above clarifies both the Government's policy and my personal views on these matters.

I consider this to be an open letter and have no objection to it being used as such.

sci.crypt: My response to a message by Dorothy Denning in 1995 – Australia and Encryption Policy

Yours sincerely

Steve Orlowski

----- End Included Message -----