

RSA[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: CRYPT-W09

The Never-Ending Crypto Wars



MODERATOR: **Bart Preneel**

Professor
KU Leuven COSIC and Tioga Capital Partners
@cosic.be

PANELISTS: **Susan Landau**

Bridge Professor in Cyber Security
and Policy
Tufts University

Erica Portnoy

Senior Staff Technologist
EFF

Adi Shamir

Professor
The Weizmann Institute

#RSAC

Law Enforcement Access: so 1990s




On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

They'll excuse us if we don't wish them luck.

SINK CLIPPER!

Because some things are better left unread. 

Copyright 1994 RSA Data Security, Inc



COSIC





We are going dark

COSIC





$$e^{\pi i} = -1$$



Laws of
mathematics
'do not apply'
in Australia

*Australian PM
Malcolm Turnbull
July 2017*

Encryption
law

Dec. 2018

RSA[®]Conference2020

Which access is needed?



Communications: voice

- telephony: phone or cell tower
- VOIP



Communications: data

- messages
- meta data



Stored data

- cloud
- media (USB)



Devices

- confiscated
- remotely

COSIC



“Apply” Slide

- Doing nothing is not an option
- Engage in public policy debate on encryption
 - Talk to colleagues and broader public
 - Get in touch with policy makers
- Think about technical approaches

COSIC

