

WASHINGTON UPDATE: INTERNATIONAL CRYPTOGRAPHY POLICY AND THE OECD

RSA Data Security Conference

January 1997

San Francisco, CA

Marc Rotenberg, director

Electronic Privacy Information Center

Washington, DC

epic.org

Role of International Politics in DC

- Lawmaking by bootstrapping (“policy laundering”)
- Recent example - WIPO treaty
- Expect to see more in the 105th Congress
- Good reasons for international policy -- global issues, common problems, common solutions
- Bad reasons for international policy -- absence of domestic political consensus

The OECD and Crypto Policy

- Organization for Economic Cooperation and Development
- 29 member countries - US, Canada, Mexico, Europe, Japan, Australia
- Wide range of issues
- Well regarded
- 1981 Privacy Protection
- 1995 Information Security
- (1997 Cryptography Policy)
- Non-binding principles



OECD Expert Panel on Cryptography

- Created in Dec 95
- Chaired by Norman Reaburn (AUS)
- Several meetings in 1996 - Canberra, Paris, Washington
- Business participation - BIAC
- Privacy participation - EPIC, representative of data protection commissioners
- GILC Public Voice Conference in Paris (Sept 96)
- Guidelines completed (Dec 96)

OECD Cryptography Guidelines

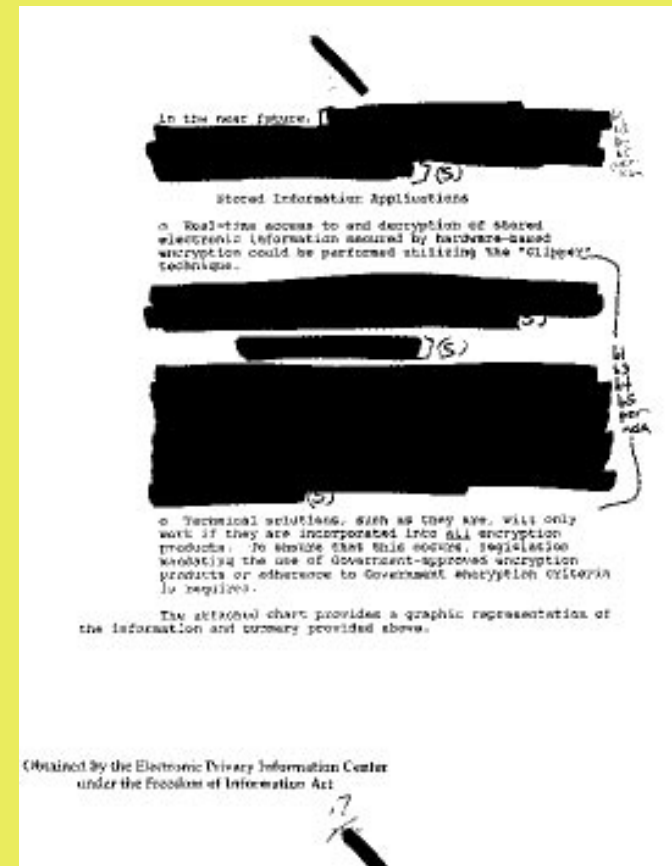
- Trust in Cryptography
- Voluntary Choice of Cryptographic Methods
- Market Driven Development of Cryptography
- Standards for Interoperability of Cryptographic Methods
- Protection of Privacy and Personal Data
- Lawful Access
- Liability
- International Cooperation

Next Steps

- Review by OECD Committee for Information, Computer, and Communications Policy (Feb 97)
- Approval by the Council of Ministers (Mar 97)
- Recommendation to the OECD countries
- OECD countries will develop policies based on Guidelines for Cryptography Policy
 - USA should move toward the OECD voluntary, market-driven model that respects privacy
 - Implications for export controls, domestic legislation and standard setting in the federal government

Reality Check: Domestic Crypto Restrictions Ahead?

- "ENCRYPTION: THE THREAT, APPLICATIONS, AND POTENTIAL SOLUTIONS" (released under FOIA 1995)
- "Technical solutions, such as they are, will only work if they are incorporated into all encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to government encryption criteria is required."



About EPIC

- Advocacy
- Litigation
- Legislation
- Conferences
- Web site and EPIC Alert
- Policy Research

“EPIC has put steady pressure on the administration concerning its policies on encryption and wiretapping.”

- *The Washington Post*

