
# Lawful Access and Security: A Transatlantic Perspective

## Workshop | 19 May 2016 | The Hague

## Discussion Background and Goals

Government organizations, companies, and individuals want to protect themselves from unwanted access to sensitive digital data. Encryption is part of the solution. At the same time, the increasing use of digital technology by criminal and terrorist organizations has heightened public concern about the threat such malicious use poses to society. Encryption can impede law enforcement's ability to investigate or prevent such crimes.

### Lawful Access to Plaintext: Not a New Issue

The controversy highlighted by FBI v. Apple is not new. In 1992, a vigorous debate began in U.S. government and industry circles about the costs and benefits of relaxing export controls on encryption products with key lengths greater than 40 bits. U.S. law enforcement and intelligence agencies opposed liberalization, while economic agencies and most of industry favored it.

In 1996, at the direction of Congress, the National Research Council prepared a study that captured viewpoints familiar today (see excerpt, right). The export control debate ended in 1998, when the U.S. allowed the export of products utilizing 56-bit DES, abandoning an earlier effort to require "key escrow" that would enable the government to decrypt information to which it otherwise had lawful access.

"For both law enforcement and national security, cryptography is a two-edged sword. The public debate has tended to draw lines that frame the policy issues as the privacy of individuals and businesses against the needs of national security and law enforcement. While such a dichotomy does have a kernel of truth, when viewed in the large this dichotomy is misleading. If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can) it also supports the national security of the United States. Framing discussion about national cryptography policy in this larger law enforcement and national security context would **help to reduce some of the polarization among the relevant stakeholders**." *Cryptography's Role in Securing the Information Society*, National Research Council, 1996 [emphasis added]

## What Is New: The International Dimension

Unlike the 1990s when U.S. encryption products dominated the market, today there is widespread access to encryption from multiple sources that is reasonably secure and user-friendly. In addition, global cloud service providers and equipment manufacturers increasingly enable encryption by default in their products. Thus no national solution can be sufficient. An international approach, comprising at least democratic nations, is required to make progress and find balance.

## Reducing Polarization: The Search for Middle Ground

Parties interested in finding solutions that will maximize security in both the online and offline worlds confront such questions as:

1. What are the economic and national security impacts of providing law enforcement with special decryption capabilities? What are the human rights/civil rights impacts?
2. How can these impacts be weighed against impacts to society when law enforcement generally cannot access plaintext?
3. Is it preferable to focus on enhancing law enforcement capabilities to utilize, where authorized, other means of getting relevant information including capturing metadata, compromising endpoints, exploiting vulnerabilities, social engineering, etc?
4. Can techniques (such as two-party (split) key escrow/key recovery systems, providing for a differential work factor, one-time software) or incentives (e.g., cost-reimbursement and/or other fees) be devised that let industry assist law enforcement without unacceptable impacts on cybersecurity?
5. What kinds of situations, events, and investigations most require speedy decryption on behalf of law enforcement?
6. What kinds of media are most important to law enforcement, e.g., information stored on a device, stored in the cloud, or in transit?

## Purpose of this Workshop

The workshop has three goals:

1. Provide updates on encryption policy developments in the U.S., Europe, and India.
2. Share viewpoints on questions such as those above. [1]
3. Identify a balanced group of experts that can work together going forward to identify promising middle ground approaches.

## Workshop Guidelines

1. The proceedings are subject to the Chatham House Rule (no attribution).
2. After a series of introductory remarks, the moderator will recognize those wishing to speak and call on them in order.
3. Participants should identify themselves before speaking, be brief, and be courteous.

1 Research on this topic is also being conducted by the Center for Strategic and International Studies (http://csis.org/program/encryption-and-government-access), report expected June 2016; and, the National Research Council (http://sites.nationalacademies.org/CSTB/CurrentProjects/CSTB_171064), report expected March 2017. The 1996 NRC study can be found at: http://www.nap.edu/catalog/5131/cryptographys-role-in-securing-the-information-society.