FITUG Statement on Crypto Policy

V 1.0a 2001-09-18

FITUG expresses its deepest sympathy for the victims of the heinous attacks in the U.S.

FITUG calls upon the governments around the world to ensure combating of terrorism and other forms of crime by proper law enforcement on the basis of law and justice in order to protect those basic values constituting a free and democratic world.

The tragic events have sparked off an increasing debate on legislative measures suitable to help preventing future acts of terrorism, in particular with regard but not limited to potential future casualties including utilisation of weapons of mass destruction (WMD).

One option recently proposed by various circles concerned comprises a re-strengthening of the signal intelligence (SIGINT) capabilities of the intelligence services and measures to facilitate the communication eavesdropping of law enforcement agencies in order to be able to uncover and monitor communication links of distributed groups of terrorists or other criminals. When following this argumentation, the availability of strong "uncrackable" encryption products to everybody can be identified as a major obstacle blocking further progress in anti-terrorism and anti-crime policy.

Such view is, however, misleading, and any resulting legislative activity based thereon will inevitably fail to reach its goal but instead undermine the basic values of freedom and democracy which we all do need to protect against terrorism in these grievous times.

In particular, **FITUG** issues a number of observations as set out below:

- Over-reliance of intelligence services and law enforcement agencies on technology-based surveillance may well lead to a lack of awareness of relevant facts. It has come to be known that frequently in terrorist or other criminal groups some of the most important information is relayed non-technologically, often carried by human couriers. Oftenly, the communications methods employed by such organisations are designed to defy technological surveillance.
- Hence, the proper way to enhance the capabilities of the intelligence services and law enforcement agencies is to effect a major reform of these institutions,

abandoning contemporary visions of defeating terrorism and other crime by monitoring the outside world by masses of officials staring on countless computer screens installed within high-security fortresses and displaying data gathered by SIGINT techniques. The SIGINT hubris has to be stopped. What the services actually need isn't more and more electronic access to private raw information but more brain power in order to derive proper conclusions. Let them then get out to mess with real terrorists and other criminals in real life. This is where a solution of the current crisis can be found.

- Cryptography is now well established as a basic technology for countless products in the emerging Information Society and, hence, a total ban thereof is deemed to be completely infeasible. Moreover, in the late 90ies of the past centuries many recognised experts in the field of cryptography have demonstrated that mandatory Governmental Access to Keys (GAK) is not a real option on a technical level; countless technical problems of large-scale GAK systems are still completely unresolved.
- Some have said that the tragic events in the U.S. are an example of high-tech terrorism. This is completely wrong. Although the captured planes surely are high-tech, the way of capturing them by rogue brutality exercised with knifes is absolutely low-tech. By no means society should forget that there is a real risk of a very severe high-tech assault on the data networks of the wired world. However, widespread use of strong cryptography is a crucial brick in a framework to protect the sensitive technical network infrastructure of the Information Society against attacks. Obstruction of free usage of strong cryptography means irresponsibly weakening the infrastructual framework of the emerging Information Society.
- Last but not least, the right to privacy of the ordinary citizen is one of the core values of a free democracy. Destroying the technical basis for preserving privacy in the Information Society means to deteriorate one of the essential characteristics of the free world.

Whatever legislative steps are taken in response to the recent attacks, terrorists and other criminals will come up with effective techniques to conceal what and with whom they communicate from where to where, or even whether they communicate at all. Thus, if legal restrictions are placed on the privacy permitted by the IT infrastructure, only criminals will enjoy unrestricted privacy.

In the current situation, law enforcement agencies should only be allowed and enabled to exploit security weaknesses of IT systems still present on the basis and within the limits of an explicit warrant issued by a competent court. No duty to implement additional weaknesses should be imposed by legislation whatsoever.

Therefore, **FITUG** rejects all attempts to impose upon the citizens any restrictive regulations of cryptography, i.e. in particular, but not limited to, by demanding GAK schemes. Moreover, FITUG urges all policymakers as well as all relevant NGOs in

this field

- to support any suitable measures to stop the current SIGINT hubris,
- to support development of alternative effective measures to strengthen societies against the threats of terrorism and other crime, and
- to strongly oppose any proposals to impose restrictive regulations upon encryption utilisation.

About **FITUG:**

FITUG creates connections to the virtual world of new media and data networks. From our statues: "The association's purpose is the fostering of the integration of new media with society, public education about technologies, risks, and perils of these media, and the fostering of human rights and consumer interests with respect to computer networks." For more information see on-line under http://www.fitug.de/

FITUG is member of the Global Internet Liberty Campaign (GILC); see on-line under http://www.gilc.org/

* * * * * * *