

Comments on Legislative Proposals to Protect National Security and their impact on the Communications Infrastructure

Computer Professionals for Social Responsibility
contact cpsr@cpsr.org Susan Evoy 650 322 3778

INTRODUCTION

Computer and communications issues have figured prominently in discussions of legislative proposals made in response to the September 11 terrorist attacks. A review of our security measures is an important part of our country's response to recent events. Unfortunately, many of the measures that have been proposed may involve significant impositions on privacy and individual liberty while possibly failing to provide meaningful assistance to law enforcement activities. Of particular concern are legislative proposals involving increased internet surveillance, computer crime, and the use of encryption.

Elements of proposed legislation in the PATRIOT bill:

Surveillance: The PATRIOT act (section 101) greatly increases the law enforcement authority to monitor electronic communications. Among other effects, it appears to lessen the need for showing due cause in obtaining court orders, instead relying more on enforcement agency discretion. It also allows for broader and less defined ways to monitor these communications.

Computer Crime: The PATRIOT act (section 309) includes "fraud, theft, or extortion related to computers" as terrorist acts. This overly broad definition risks classifying a wide class of acts as potentially subject to life imprisonment, according to the terms of section 309.

Encryption: Concern over the use of encryption technologies has led to the revival of calls for key escrow or recovery systems. Law-enforcement efforts would certainly be aided by tools that could be used to read private communications between terrorists, but the widespread availability of strong encryption would make escrow or recovery moot. These proposals would limit the effectiveness of legitimate tools that provide infrastructure security through encryption, while terrorists with the use of numerous simple and hard-to-detect tools such as one-time-pads and steganography.

CPSR is a public-interest alliance of computer scientists and others concerned about the impact of computer technology on society. We work to influence decisions regarding the development and use of computers because those decisions have far-reaching consequences and reflect our basic values and priorities. Since its founding in 1981, CPSR has

worked on a wide range of issues, including encryption technology, and the Y2K computing bug and disaster recovery.

Critique of Some Points of Proposed PATRIOT Act:

SURVEILLANCE: The PATRIOT Act could be construed to include in its definition of permissible activities the use of technologies such as Carnivore to sift widely through public electronic communications looking for something of interest. This technology could be used to monitor all communications in the country, or through a service provider, looking for patterns of interest. The details of this proposed device have been kept secret. It is important not to grant broad approval of such activities that are beyond scrutiny and for which there are not standard checks and balances. To avoid this pitfall, section 101 should more closely define pen registers and trace and trap devices for electronic communications as to the size of the net they're allowed to cast, and what they can gather.

Blanket monitoring of all citizen communications seems inadvisable. One of the goals of terrorism has been stated to be having a chilling effect on democracy, and on society in general, creating fear and limiting normal activities such as travel and communications. Blanket monitoring of all citizens would seem to accomplish that negative goal. In addition it will undoubtedly drive a response in the Internet community to develop tools for encrypting all communications between all people, thus guaranteeing a much harder job for law enforcement when it has a valid wiretap order.

COMPUTER CRIME

The PATRIOT act's definition of terrorism includes "fraud, theft, or extortion related to computers". This overly-broad definition may be interpreted as applying to a wide range of activities, including:

- Sales and distribution of software that fails to perform as advertised
- Provision of potentially incorrect or misleading content on web pages.
- Internet-based multi-level-marketing schemes

The use of the term "theft" in this context is particularly troublesome. The use of computer technology to steal monies or valuable digital information should certainly be a crime, but it is not necessarily terrorism. Similarly, denial of service (DOS) programs that block access to web servers might be seen as somehow "stealing" computer cycles or other resources, but are not in all cases necessarily an act of terrorism.

Computers certainly have the potential to be powerful tools for skilled terrorists. Attacks on computer systems might be used to cripple communications infrastructures, interfere with financial markets, or steal corporate or government secrets. When conducted with the clear intent of causing terror, these actions should be considered terrorism. However, the generality of the language found in the draft PATRIOT act raises the possibility of disproportionate sentences for less serious computer crimes.

ENCRYPTION

The worldwide availability of strong encryption algorithms and software is a difficult fact of life. It is important to allow appropriate government agencies authority to crack encryption under the correct wiretap authority. However, some would make encryption illegal, thus crippling many authentic applications. Other proposals would make encryption research of doubtful legality since it includes the necessary investigation into whether encryption methods are vulnerable by trying to crack them. We have already witnessed some erosion in world prominence in encryption by limiting research and export of encryption.

Other proposals call for government agencies to hold back door keys on encryption. Studies have been made on abuse by law enforcement agencies of government databases of private data on citizens; it is not unthinkable that legitimate private communications including commercial transactions of considerable size could be compromised.

In fact key escrow could easily be exploited by terrorist organizations and corporate espionage agents, since it takes the security offered computer technology claiming to be impenetrable and reduces this security to whatever can be had with administrative workers in government bureaucracies. Furthermore, key escrow systems require key repositories which would themselves be enticing targets for terrorist attacks.

Strong encryption is also vitally important for the secure systems that will be needed to protect crucial electrical, communications, and financial networks. Key escrow measures that make decryption easier for law enforcement efforts will limit efforts to prevent attacks on critical infrastructures.

CONCLUSION

CPSR shares in the national concern over the possibility of further terrorist acts. However, we are concerned about the possible impacts of legislation that is overly broad in its language and unclear in implementation. Any legislation that is adopted should balance concerns with security and law enforcement against concerns regarding legitimate uses of technology, privacy, and other civil liberties.

References:

EPIC analysis of PATRIOT Act: http://www.epic.org/privacy/terrorism/patriot_sec.pdf |

The Risks of Key Recovery, Key Escrow, & Trusted Third Party Encryption
<http://www.cdt.org/crypto/risks98/> |

Dahl, Mary Karen. The National Crime Information Center: A Case Study in National Databases, (Palo Alto, CA: Computer Professionals for Social Responsibility, March 1988), 4 pages.