# GOVERNMENTAL ACCESS TO ENCRYPTED INFORMATION
## *To What Extent and How to Achieve that Extent?*

Hamid Turab Mirza
*Department of Computer Engineering, College of Electrical and Mechanical Engineering*
*National University of Science and Technology, Rawalpindi, Pakistan*

Keywords: Cryptography, Government Policies, Free Society.

Abstract: No body can deny the importance of encryption technology in today's communications, with all the benefits it has also posed some threats, due to which, governments and regulatory bodies have great concern about encrypted information and have set out some policies and are still busy in regulating the wide spread use of encryption technology. In an attempt to control the encryption technology to make the society safe from the threats of terrorism and crime, governments have over shadowed the benefits of encryption technology for the privacy, liberty of the citizens and economic growth of the nation. There has been a lot of opposition and criticism on these policies, and society has objected to the demands of governments over encryption technology, and have demanded balanced solutions that should take safety within the context of free society and not otherwise.

## 1 INTRODUCTION

"Encryption is a process of turning normal text into a series of letters and/or numbers which can only be deciphered by someone who has the correct password or key" Eden (2000:361). Mankind has been using encryption since at least the time of Pharaohs. It has been used for hiding messages and important private information. Although for long encryption has been associated with the military and governments only, but today, ordinary citizens, financial institutions, international businesses use encryption on regular basis (Gaver, 2000).

In 1970's when international financial Industry became more automated, only then the importance of encryption in business communication was recognized, before that until recently this technology was thought to be an exclusive domain of governments (Barth and Smith, 1997). Today all businesses use technology and have their sensitive business information and trade secrets online and the desire to keep it secret and safe from the prying eye is quite natural. In today's world encryption technology is fundamental for the development of global electronic commercial systems. Akdeniz and Walker (2000) state that other than the industry encryption is also serving the humanity, organizations such as Amnesty International and Human Rights Watch communicate with dissidents all around the world with the help of encryption technology.

## 2 WHY GOVERNMENTS WANT ACCESS TO ENCRYPTED INFORMATION?

As nations are becoming more and more dependent on communication technologies the chances of the exploitation of these technologies by the high-tech criminals is a major threat to the public safety (Walker et al, 2000). Since the beginning governments have been interested in regulating encryption technology for the two core reasons, national security and law enforcement, military is concerned with the first and police with the second (Barth and Smith, 1997).

More specifically with the emergence of World Wide Web (www), now people all over the world can exchange information freely and easily regardless of any boundaries; Hence the excesses of the cyber space and the use of encryption technology are viewed as threatening by the authorities and it is felt that there is a need for regulation of this space but one of the main problem faced by the regulatory authorities is; that there is no overall ownership of



Turab Mirza H. (2008).
GOVERNMENTAL ACCESS TO ENCRYPTED INFORMATION - To What Extent and How to Achieve that Extent?.
In *Proceedings of the Fourth International Conference on Web Information Systems and Technologies*, pages 467-473
DOI: 10.5220/0001531604670473

the internet, however it is not the case that currently there are no laws and regulations in place or that no future laws can be devised to govern the internet, (Walker et al, 2000; Wall, 2001) emphasize that even if it was ever a wild west frontier then it has been tamed very quickly and by looking at the number of users and complexity of the Internet activity it is still remarkably ordered.

With the increase in use of strong encryption technologies governments are feeling that they will loose their control and will not be able to do the surveillance as they were doing before. The remarks that: "Encryption is here and it's going to grow very rapidly. That is bad news for Sigint" (Signals Intelligence) given by the head of staff of the US House of Representatives Permanent Select Committee on Intelligence, ex CIA officer John Millis to CIA veterans give very clear indication of the government fears (Cyber-Rights & Cyber-Liberties, 2000).

Eden (2000) points out that, the fact that encryption can also lead to help the criminals hide their activities has raised a voice that cryptography providers should deposit encryption keys with some trusted third party, in this regard different governments have adopted different policy approaches in effort to contain the threats posed by encryption. Barth and Smith (1997) state that, encryption can be mainly controlled in three ways that are import control, export control and use control.

# 3 ENCRYPTION POLICIES OF GOVERNMENTS

## 3.1 UK Policy

The UK government has been trying to formulate a policy on encryption since 1994, but there had been many policy twists and turns over the time, the core reason behind this is the difference of views of the two governments before and after the general election May, 1997, EU and OECD policies also played a role in the delays (Akdeniz and Walker, 2000).

Government has proposed Key recovery encryption system, it provides a way to access the plain text without going into the formal process of encryption and decryption; in recent years many encryption systems like key escrow, trusted third party (TTP), exceptional access, data recovery and key recovery have been introduced. Abelson et al (1998) identifies that although each of these systems has its own mechanism but overall all of them serve the same purpose of assuring third party (government) access to encrypted data.

In the beginning British Government was also planning to implement the 'key escrow' the same concept of depositing the key with trusted third party. But due to strong opposition of the business community, the Electronic Communication Act 2000 abandoned 'key escrow' in UK (Eden, 2000). Also there was also a proposal about licensing of Trusted Third Parties (TTP's) who will be holding the copies of all encryption keys to facilitate recovery and verification (Akdeniz and Walker, 2000). The Regulation of Investigatory Powers Act (RIPA) allows law enforcement agencies that; they can have access to the communication data for broad range of purposes without even obtaining a court order (Jayasekera, 2001).

Abelson et al (1998) states that although there had been a lot of opposition of these policies and proposals, but government justifies them that these systems have associated benefits such as if some user lost the key then it can be recovered through the TTP, otherwise user faces the risk of loosing the crucial data in case of normal strong encryption.

## 3.2 US Policy

Since the beginning U.S.A. has been on the forefront of policy making on encryption technology, fighting cyber crimes was one of the major issue mentioned in President Clinton's 1999 "State of the Union" message, it also mentioned the need for the battle over encryption and the need for the law enforcement and intelligence agencies to retain access to telecommunications with out the need for slow and expensive decryption, Levi (2001) points out that same is mentioned in the United Kingdom's Regulation of Investigatory Powers Act (RIPA) 2000.

Over the time U.S has reconsidered its policies, according to The Center for Democracy and Technology (2001), On January 14, 2000 the U.S. government published new encryption export regulations, which made it much easier for the companies or the individuals in the U.S to widely export strong encryption regardless of how strong the encryption is. However the new rules do not decontrol the encryption and still there are a lot of concerns about privacy and free speech. There were some very catchy rules in January 2000 regulation rules like, encryption products can be exported to any, but few nations on U.S. "Terrorist" list, where

as encryption products having less than 64-bits can be exported freely.

In light of these relaxations Akdeniz and Walker (2000) predicted that in future encryption software will become a standard part of the common use software's, this idea has already been transformed into reality as Microsoft Windows 2000 incorporates 128-bit encryption, specifically permitted by relaxed US government regulations on encryption exports announced in January 2000. Overall U.S governments efforts to stop the wide spread use of encryption technology both inside and outside U.S. has been pretty successful, Schneier and Banisar (1997) doubt that this success might be short lived.

### 3.3 Various National Policies

Other governments in the world are also considering the laws and regulation about encryption technology, but few have implemented it well where as others have completely ignored this issue, French Government took a dramatic turn away from encryption controls when Prime Minister Lionel Jospin announced on 19th January 1999 that France was dropping its long held restrictions on use of cryptography where as Irish government has already rejected internal and export controls in June 1998, Japan on the other hand is financing the research and development of encryption technology (Barth and Smith, 1997; Akdeniz and Walker, 2000). According to EPIC's report, Cryptography and Liberty 2000, only Malaysia and Singapore have existing laws mandating lawful access to encryption keys, similar to the approach of UK's RIP Act.

Other than these policies governments are also involved in secret global surveillance. A report by American Civil Liberties Union (2004), mentions that there exist very powerful systems like ECHELON and ENFOPOL that collect data in several ways, whereas governments have not yet accepted their existence.

## 4 WORLD VIEW: CONCERNS ABOUT GOVERNMENTAL ENCRYPTION POLICIES

The internet society is considered to be a free society, where people can have freedom of expression and speech regardless of all physical boundaries and constraints, few of the core principals of the Internet Society (ISOC) a non-profit, non-governmental, international club of Internet enthusiasts around which much of the constitution has resolved are: Online free expression, which is not restricted by other indirect means such as exclusively restrictive governmental or private control and free, use of encryption (Walker et al, 2000).

Since the beginning there had been a severe opposition of the policies against cryptography, as it is very much obvious that the common use of encryption technology is very much necessary for the preservation of human rights in the Information Society but today many law enforcement and Intelligence agencies are trying to redesign communication networks to ensure the easy and effective surveillance from their desktops, Schneier and Banisar (1997) further say that these kinds of proposals would be more suited for the old Soviet Union then the free world.

Currently we are witnessing a governance system and shadows of political impacts on these liberties, especially governmental policies have been crucial to control technologies such as cryptography, which is an essential part of the e-commerce and other kinds of security mechanism over the net. These kinds of policies will have a major impact on the development of e-commerce. Barth and Smith (1997) share the same view that strict controls on encryption technology will harm those industries that stand to benefit from the booming demand of information security, by looking at the advancements in technology and the way global market reacts to it, one can easily predict that governmental controls which are ineffective today will become irrelevant tomorrow and strong encryption is going to be the core component of the international infrastructure for electronic commerce and keeping in view this fact that different governments have different encryption policies, it is very much clear that the economy of the specific country with tight regulations will drastically suffer.

In the same way current UK government specifications of the key recovery system, diverge many ways from the needs of individual or commercial encryption users, for example Demands of Law enforcement to have a real time 24-hour-a-day, 365-day-a-year access to plaintext, access to the keys without the end-user knowledge or consent, the efforts to implement key recovery system to the this extent will slow down the development of the e-commerce (Abelson et al, 1998), also the U.S clipper proposal got immense opposition from public. A Time/CNN poll of 1000 people, conducted in March 1999 found that 80% of people strongly opposed the proposal when it was described to them. Another

electronic petition organized by the Computer Professionals for Social Responsibility (CPSR) that was asking President Clinton to withdraw the Clipper proposal gathered nearly 50,000 signatures, including many of the world's prominent computer security and cryptography experts (Schneier and Banisar, 1997).

These kinds of proposals have been highly opposed both by the civil libertarians and the industry, these policies are against the basic human rights and are a direct attack on the privacy and civil liberties, which are necessary for an open society in an electronic age and privacy should not be taken as secrecy (Silverman, 2000; Hughes, 2001), but today governments have developed very very large databases (VVLDB's) and have become custodians of information that can very much affect the lives of individual citizens and there had been many cases of misuse of these data banks, Martin (1998) sees this kind of surveillance as a serious and growing social issue and stresses that root of this problem is unequal power, he also makes a point that all these proposals like key escrow and trusted third parties require the cooperation of the industry and citizens and without their cooperation there is no way that these proposals can be implemented.

Martin (1998) further states that surprising it may seem surveillance depends on cooperation by the person who is under observation. Hence there is a need for spreading mass awareness among people so that they can protect their privacy and liberties while communicating in their daily life, Zimmermann (1995) Creator of the most popular and controversial encryption software PGP (Pretty Good Privacy), sees advancements in this field as a seed crystal for the growth of Crypto Revolution, and terms it as new political movement for civil liberties in the Information Age.

# 5 NEED FOR A BALANCED APPROACH

Although it is the fact that with help to the secure communication, encryption technology also presents problems for the law-enforcement and nobody can deny the fact that there are times when law agencies need to get the private encryption keys, members of law enforcement and intelligence agencies are very right about their concerns about the usage of unescrowed cryptography, but this need has to be balanced against the rights of freedom to speech and personal privacy (Akdeniz et al, 1997; Abelson et al, 1998) and there is also a a risk that the efforts of the governments to implement a key recovery system will increase the risk of crime and information terrorism instead of decreasing it. The increase in number of people having access to this central key repository will maximize the chances of corruption even if it's by a mistake.

Abelson et al (1998) further emphasize that a huge network linking number of law enforcement agencies with different key recovery centers, requires extraordinary level of human trustworthiness hence will be difficult to secure and will be much more vulnerable to attackers. Looking at the complex nature of the problem and the difference in policies of the governments, due to the lack of balance between security and liberty, countries such as Sweden, Germany and United States have been called as surveillance societies but on the other hand many governments notably in Scandinavian countries consider it as a tool and don't control it, same is the case with developing countries. Barth and Smith (1997) express their fears that, these countries are safe heavens for cyber criminals, free from any regulation and are threats to the whole international effort of containing the spread of strong encryption, so in the light of these facts it is predicted that internationally accepted encryption standards will merge together and eventually will sidestep the government control on export, import and use of encryption technology. This way together these developments will doom the efforts of individual governments to prevent the secure communication both locally and internationally.

Looking at the problems with these proposals Schneier and Banisar (1997) predicted that ultimately these proposals will not be as effective as the Federal Bureau of Investigation (FBI) and National Security Agency (NSA) assert because most criminals will simply adopt more secure alternatives, Barth and Smith (1997) share the same view that, as the cost of computing power goes down, demand for the strong encryption will definitely increase, ironically the main affect of the government policy might be an increase in crime.

On the other hand it is also argued that encryption technology is not that big threat and governments are just using it as a tool to increase and justify their surveillance powers, according to a Townsend & Taphouse (1998) it has been noticed that respected people from U.S. Government are giving some misleading statements about encryption, according to them cracking DES (Data Encryption Standard) is much more difficult and

thousands of computers will take weeks and years to crack a single message. Where as according to cryptography research community 40-bit RC-4 encryption can be and has been broken by a group of students. Even the security of 56-bit DES is in doubt; a private sector report claims that a computer system costing $ 10 million can break any DES encryption in six minutes (Barth and Smith, 1997).

So there is a severe need to have a balance between the policies as security expert Bruce Schneier said in his interview to Barrett (2004) a News Week reporter, that he sees the need to have a more balanced approach toward security, as it is just one of the goal of the country, and further said that if we lock every person in the country then it will be very secure but unfortunately that wouldn't be a better society.

# 6 COMPROMISED PROPOSALS: HOW TO ACHIEVE THE RIGHT EXTENT OF ACCESS

There had been a lot of discussions on the need for surveillance and the control of encryption, many proposals by different governments have been presented but all of them are mostly on one extreme that is stress on national security and law enforcement, that reason being that these proposals are not accepted widely is, these proposals do not take into account the privacy, freedom of speeches and liberties of a net citizens.

According to Martin (1998) surveillance is not a new problem, but invasion of privacy by large remote organizations is quite new. Encryption is just a technical solution to anti surveillance but he emphasizes that unless the society accepts it, technical solutions are of no use. The awareness about the privacy is constantly on the rise and people have high concerns about the privacy of their data over the networks, (France, 1998) suggests that data protection supervisory should be developed to play a role in providing those safeguards, which common citizen is entitled to under the Data Protection Act (DPA) 1984. This fact has been recognized by the authorities and they have agreed that trust worthy providers of the cryptography are very much important for the growth of the e-commerce, and that commercial organizational information must be saved against both commercial and state sponsored surveillance (Barth and Smith, 1997; Eden, 2000).

Akdeniz and Walker (2000) point out that the major problem faced here is that who can be trusted? to build the trust in information age, a Regulatory framework must be established at a national, supranational and international level. The fact that there is a considerable difference between EU and US policies, and even the conflict of policies in between EU members like UK and France is alarming. The absence of consensus hampers not only the growth of e-commerce but also diminishes the dream of netizens to have a stable and trustworthy environment in cyberspace.

On the other hand Martin (1998) proposed an extremist solution for eliminating the surveillance, he suggests if there is a need for surveillance of a nuclear reactor than the solution is to abolish the reactor, further he adds that organizations such as FBI, MI5 and KGB should seize to exist, as spy agencies have probably done more to promote than to prevent terrorism.

Abelson et al (1998) observed that in spite of all the efforts and research still neither industry nor government has been yet able to produce a key recovery system that satisfies all requirements. Barth and Smith (1997) also support the view that there are a lot of loopholes in policies and only prospect for effective governance is a tightly coordinated international policy coupled with national enforcement, it is further emphasized that governments will have to take some concrete decisions very quickly, by looking at the rapid advancements in the area of cryptology any effort of policy making at international level might be too late. In this regard many scholars and renowned security and social liberty experts have proposed some solutions which can be termed as compromised solutions which take both security and social liberty into account.

It is pointed out by Akdeniz et al (1997) that crime prevention is one requirement and it should be considered with in the context of the encryption debate and should not over shadow it. They suggest a compromised proposal to avoid the both extremes in encryption policy and the breach of privacy by the governments. They propose a solution of 'Key Archiving', which recommends that citizens and organizations to archive the keys with themselves, the archive copy will only be recoverable from trusted third parties (TTP) when the key has been invalidated against all subsequent use. Most importantly in this solution user will always know that the key has been compromised or revealed to the authorities, this might help to avoid the misuse of keys from those who do not have the proper authority.

Akdeniz and Walker (2000) favored a 'zero option', which suggests that governments should

adopt alternative approaches to policing, as criminals cannot be completely prevented from having an access to strong encryption and bypassing the escrowed encryption, on the other hand extreme policies will have drastic affect on the developmental policies of the government to make Britain a liberal society, a favorable location for e-commerce and network development.

# 7 CONCLUSIONS

In this Information Age no one can deny the benefits and importance of encryption, due to advancements in technology the way people communicate has changed and it is necessary that this communication should be secure, encryption technology is used for the same purpose. Today business and citizens highly rely on the encryption technology for the reliable communications, but with all the benefits encryption has also posed the threats, fears that criminals can also use the same technology for carrying out their crime and it could be to the extent of national security. Due to these threats governments have shown their concerns and are busy in developing policies and regulations to control the wide spread of strong encryption, so that they can intercept any communication when ever they want to. For this reason different governments have passed different regulations, these regulations allow enforcement agencies to access or intercept any communication or data. Apparently the reason behind this is national security and law enforcement for the public safety.

These regulations and proposals have a lot of problems and loop holes, which have been highly criticized by many societies. According to those regulations every body using the strong encryption software should submit his keys to some trusted third party from which government or law enforcement agencies could get the key and access the private or confidential information without the knowledge of the owner of that information or data. This is clearly against the liberty and privacy rights of the citizens, and will make the whole communication system insecure for commercial business in specific and private users in general.

Society has reacted to these demands of governments to have access to private, confidential information to this extent. It has been argued that these policies are only taking in account the national security and demands of law enforcement agencies and are overshadowing the basic concept of liberal and free society. Hence it is demanded that there must be some balanced approach to this issue, which is acceptable for the citizens, industry and governments.

# REFERENCES

American Civil Liberties Union. (2004). “Echelon Watch”. American Civil Liberties Union. [Online]. New York: ACLU, American Civil Liberties Union. http://archive.aclu.org/echelonwatch/faq.html

Akdeniz, Y. and Walker, C. (2000). “Whisper who dares: encryption, privacy rights and the new world disorder”. In: Akdeniz, Y., Walker, C. and Wall, D. (ed.), The Internet, Law and Society, pp. 317-348. Longman, 2000.

Abelson, H., Anderson, R., Bellovin, Steven M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, Peter G., Rivest, Ronald L., Schiller, Jeffrey I. & Schneier, B. (1998). “The Risks Of ‘Key Recovery,’ ‘Key Escrow,’ And ‘Trusted Third-Party’ Encryption”. Center for Democracy and Technology. [Online]. Washington : Center for Democracy and Technology. http://www.cdt.org/crypto/risks98/.

Akdeniz, Y., Clarke, O., Kelman, A., Oram, A. (1997). “Cryptography and Liberty: ‘Can the Trusted Third Parties be Trusted ? A Critique of the Recent UK Proposals’”. The Journal of Information, Law and Technology (JILT). [Online]. The Journal of Information, Law and Technology (JILT) 1997 (2). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_2/akdeniz/.

Barrett, J. (2004). “An Enormous Waste of Money, A security expert argues that America is spending its money ineffectively in the fight against terrorism”. Newsweek, Inc. [Online]. MSNBC: 2004 Newsweek, Inc. 17 March 2004. http://www.msnbc.msn.com/id/4549661/

Barth, Richard C. and Smith, Clint N. (1997). “International Regulation of Encryption: Technology Will Drive Policy”. In: Kahin, B. and Nesson, C. (ed.), Borders in Cyberspace: Information Policy and the Global Information Infrastructure, pp. 283-299. The MIT Press, 1997.

Cyber-Rights & Cyber-Liberties. (2000). “Interception Capabilities 2000, Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office) on the development of surveillance technology and risk of abuse of economic information Regulations”. Cyber-Rights & Cyber-Liberties. [Online]. Leeds: Cyber-Rights & Cyber-Liberties. http://www.cyber-rights.org/interception/stoa/ic2kreport.htm#Summary.

Eden, P. (2000). “Electronic commerce – law and policy”. In: Akdeniz, Y., Walker, C. and Wall, D. (ed.), The Internet, Law and Society, pp. 349-369. Longman, 2000.

France, Elizabeth. (1998). “Privacy and Openness: Data Protection, Privacy and Confidentiality”. In:

McDonald, A. and Terrill, G. (ed.), Open Government, Freedom of Information and Privacy, pp. 45-66. London: Macmillan, 1998.

Gaver, J. (2000). "Encryption: Why You Should Use it, Why the Feds Want it Stopped". Action America. [Online]. Action America: Uncommon Insight into Common Issues. 10 October 1999. http://www.actionamerica.org/privacy/encrypt.html.

Hughes, Eric. (2001). "A Cypherpunk's Manifesto". In: Schneier, B. & Banisar, D. (ed.). The Electronic Privacy Papers, Documents on the Battle for Privacy in the Age of Surveillance, pp. 285-287. John Wiley & Sons, 1997.

Jayasekera, R. (2001). "Internet: Mass surveillance, Bug them all and let Echelon sort them out". Index on Censorship. [Online]. Index on Censorship: for free expression. 8 November 2001. http://www.indexonline.org/news/20011108_europe.shtml.

Levi, M. (2001). "Between the risk and the reality falls the shadow, Evidence and urban legends in computer fraud (with apologies to T.S. Eliot)". In: Wall, David S. (ed.), Crime and the Internet, pp. 44-58. London: Routledge, 2001.

Martin, B. (1998). Information Liberation, Challenging the corruptions of information power. London: Freedom Press, 1998.

Silverman, Debra L. (2000). "Freedom of Information: Will Blair be Able to Break the Walls of Secrecy in Britain?". In: Vaughn, Robert G. (ed.), Freedom of Information, The International Library of Essays in Law & Legal Theory, Second Series, pp. 351-433. Ashgate Pub Co, 2000.

Schneier, B. and Banisar, D. (1997). The Electronic Privacy Papers, Documents on the Battle for Privacy in the Age of Surveillance. John Wiley & Sons, 1997.

The Center for Democracy and Technology. (2001). "U.S. Encryption Policy, Current Encryption Export Regulations". Center for Democracy and Technology. [Online]. Washington : Center for Democracy and Technology. http://www.cdt.org/crypto/admin/.

Townsend & Taphouse. (1998). Politics of Decryption, TECS, Intelligence Papers, Cracking DES [Online]. Townsend & Taphouse. http://www.itsecurity.com/papers/crackdes2.htm.

Wall, D. (2001). "Maintaining order and law on the Internet". In: Wall, David S. (ed.), Crime and the Internet, pp. 167-183. London: Routledge, 2001.

Walker, C., Wall, D. and Akdeniz, Y. (2000). "The Internet, law and society". In: Akdeniz, Y., Walker, C. and Wall, D. (ed.), The Internet, Law and Society, pp. 3-24. Longman, 2000.

Zimmermann, Philip R. (1995). The Offical PGP User's Guide. The MIT Press, 1995.