II

# PROGRESS IN SECURING THE GLOBAL

B R Gladman

**Rapporteur:** Rogério de Lemos

# PROGRESS IN SECURING THE GLOBAL INFORMATION INFRASTRUCTURE

**Dr. Brian Gladman**[1]

This paper presents the personal views of the author and not those of the organisation for which he works.

## Introduction

Over the last few years the Internet has grown at a phenomenal rate to create a global network infrastructure spanning some 30~50 million people in more than 100 countries. By its very nature the Internet is an open and insecure infrastructure but applications are now emerging which require confidentiality, integrity and authentication if they are to operate effectively.

The World Wide WEB in particular promises to progressively transform the Internet from a low level network into a truly global information infrastructure carrying a wide range of commercial services for which security and integrity will be essential requirements.

The Internet is not a managed infrastructure but rather a very large number of individual links and computer nodes which are loosely federated to create a richly interconnected network. These links and nodes are physically located in many different countries and are owned and operated by thousands of different organisations who co-operate in an informal alliance to provide a common set of end-to-end services using agreed protocols and standards.

The way messages are handled by the Internet can be likened to the handling of letters in the global postal service. Users send and receive letters using local post boxes, leaving it to postal services to organise the movement of these letters between the senders and the recipients. The Internet works in the same general way with users sending and receiving messages via their local connection points; the computers at the nodes in the network then co-operate with each other in order to move these messages across the network between the senders and the recipients.

There is, however, one major difference between the Internet and the postal service – messages on the Internet are put in transparent envelopes which allow the contents to be read anywhere in the network!

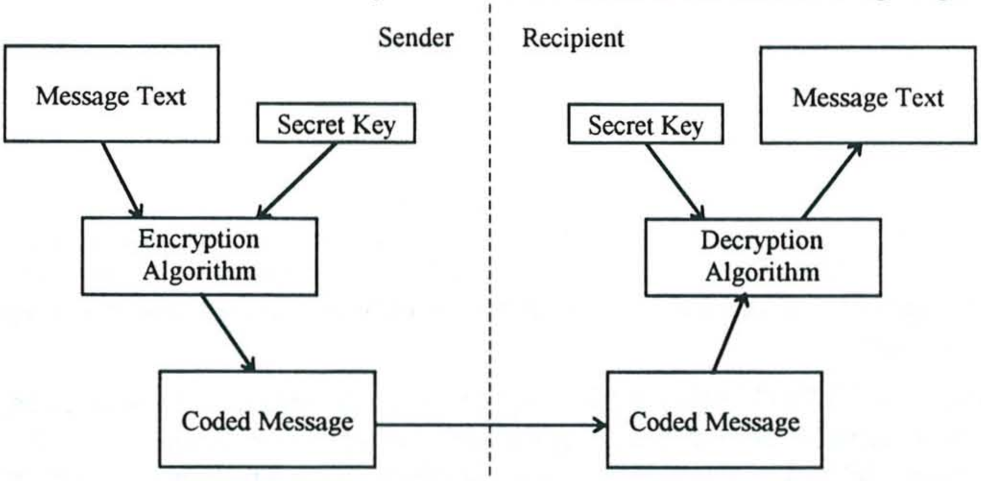
In order to overcome this problem an electronic equivalent of opaque envelopes is needed so that the contents of messages cannot be seen within the network infrastructure. In fact a technology capable of providing this – cryptography – exists but political factors have severely constrained its widespread use.

This paper provides an overview of the use of cryptography to provide security in the global information infrastructure and discusses the political factors which have limited its application. It looks in particular at activities which are being pursued at the moment to promote its wider application.

[1] currently Deputy Director of The SHAPE Technical Centre, The Hague, The Netherlands

### Secret Key Cryptography

In secret key cryptography a message is coded by mixing it with a secret key which is known to both the sender and the recipient. This is illustrated in the following diagram.



Because both the sender and recipient need to know the secret key a safe and secure method of passing this between them is needed. This can be done if a secure means of communication is available but if this is the case we could use this to send the message in the first place.

In practice secret key cryptography is still useful because the keys can be exchanged by manual means. Nevertheless this is an expensive and time consuming process and this has meant that this form of cryptographic protection has only been extensively used by governments and large organisations.

### Public Key Cryptography

In 1978 Rivest, Shamir and Adleman published a paper[2] which was to prove a turning point in the protection of the global information infrastructure. Their approach, known as RSA, allowed the protection of messages using keys which could be made public!

The approach is most easily explained using an analogy with special safe boxes each of which have two unique keys. When a box is closed with one of these two keys it can only be opened with the other and vice versa.

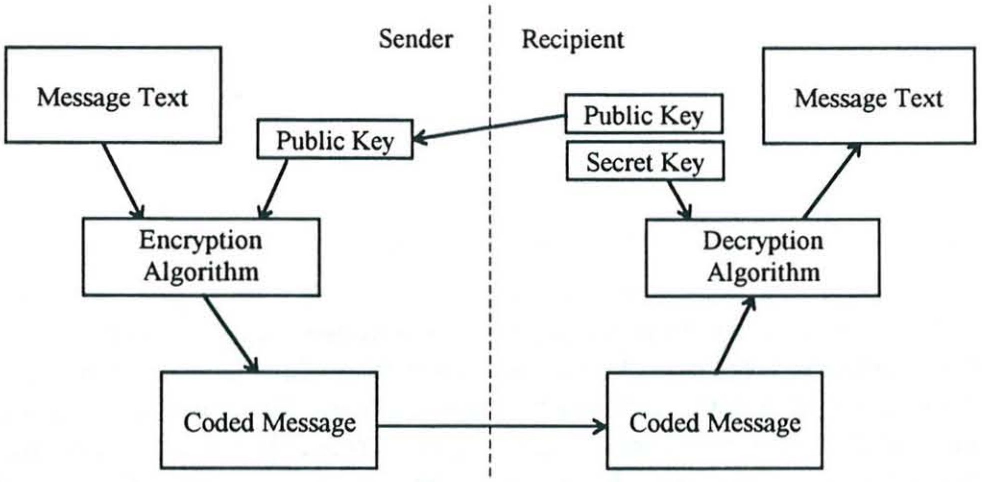
A person can use these boxes to receive secure messages in the following way. First of all they hide one of the two keys and then get a locksmith to make many duplicates of the other which they then give to their friends (they also give them safe boxes). When their friends want to send a message to them they put it in the supplied box, close it with the supplied key and then post it to them. Since the originator's hidden key is the only one which can then open the boxes, only they can read the message – once they have closed the boxes not even the senders can do this!

In order for this to be safe the people sending the messages have to be sure that the keys they use really belong to the person to whom they want to send a message. Otherwise someone could send them a key from a different pair and pretend to be this person. To overcome this the locksmith who makes key copies can check the identity of the requester

[2] R.L. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, 21(2): 120-126, February 1978

and issue certificates that the keys are genuine. For electronic keys these are known as public key certificates.

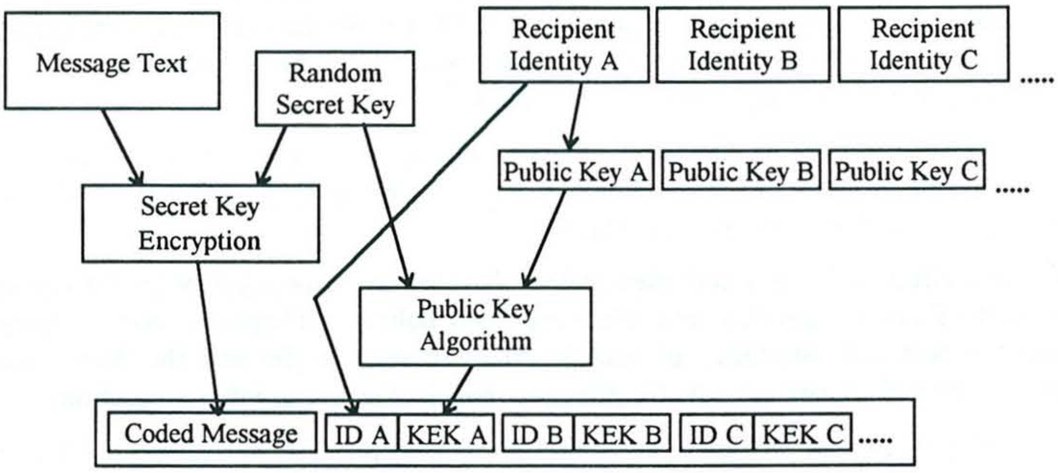
In its electronic form this scheme thus works in the following way.



The scheme also provides a way of making an electronic signature. Using the safe box analogy again, if a person wants to sign a message they put it in a safe box and lock this box with their secret key before sending it to the recipient with their name on the outside. When the recipient gets it they select the public key for the person named on the outside and unlock the box. If this works they can be confident about the sender since only he had the secret key which could lock the box in such a way that his public key opens it. In effect, therefore, the sender has signed the message.

### Protecting Messages in Practice – The Hybrid Scheme

In fact public key methods are very inefficient and slow when compared with secret key approaches but a method exists which combines the best of both worlds as follows.



Here the message to be sent is first coded with an efficient secret key method using a randomly generated secret message key. This key is then encrypted using the public key of the first recipient and the result (KEK) placed with their identity in the message header. This is repeated for each recipient and the whole message is sent to each of them.

Recipients first scan the header for their identity and then use their private keys to decrypt the KEK field to give the secret message key. They then use this to decrypt the message.

This scheme provides a practical and effective mechanism for providing end-to-end message security in the global information infrastructure. It can also be extended as already indicated to achieve electronic signatures and hence provide a basis for end-to-end authentication.

This hybrid approach is used in the Internet 'Privacy Enhanced Mail' standard.

### Political Factors In The Exploitation of Cryptography

While many individuals and organisations have a desire for privacy in their use of the Internet there are others who oppose this. These include many governments, law enforcement agencies and intelligence organisations.

The importance of code-making and code-breaking in World War II has led many governments to treat cryptography as a controlled military technology. In particular, NATO countries, Japan and Australia co-ordinate their export control laws to limit the spread of cryptographic techniques. Most countries, with the notable exception of France and Russia, do not place constraints on the internal exploitation of cryptography although even here many are not above using 'behind the scenes' means of constraining its application.

Law enforcement agencies in many countries have expressed concern about widespread use of cryptography for providing privacy. They often argue that honest citizens have nothing to fear from having their messages read and do not therefore need privacy. In practice, however, this argument is not sound since cryptographic privacy is not just about end user information but also about the protection of passwords, financial transactions, industrial and commercial information, and much other information which needs good protection.

Over recent years there have been well publicised Internet attacks using 'password sniffers' to obtain an initial entry points into network hosts. Currently much of the network user population is wide open to this form of attack and the network as a whole is highly vulnerable here. For reasons such as these most law enforcement agencies accept the need for privacy via cryptography but argue for a legal means of obtaining the keys when necessary so that messages can be intercepted.

Intelligence agencies depend heavily on reading traffic on such networks as the Internet and, not surprisingly, they are the main advocates for continuing government restrictions on the widespread exploitation of cryptography.

In the United States the activities of the National Security Agency in this respect are the subject of much vigorous and relatively open debate. There are now steadily growing tensions between the desire of such agencies to read traffic and the desires of industry, commerce and private citizens for effective means of cryptographic protection.

In Europe such groups take a lower profile than in the United States but they are no less active in seeking to constrain the spread of effective methods of cryptographic protection. It has been suggested by Ross Anderson[3], for example, that intelligence agencies in the UK and Europe have sought to constrain academic research in cryptography. He also puts forward the view that European Information Security Research is overseen by a body – the Senior Officials Group (Information Security) – which consists of signals intelligence managers who act consciously to prevent the development of any effective cryptographic protection. Further than this, he refers to comments from insiders who believe that this

[3] Crypto in Europe – Markets, Law and Policy. Ross J. Anderson, Cambridge University Computer Laboratory.

group even goes as far as approving defective projects in order to avoid funding those which are more worthy and hence more damaging to their interests.

If this is true, there is evidently a big difference between the United States and Europe in that authorities in the United States have to justify their actions in public whereas actions and policies in Europe are being pursued 'behind the scenes' in an invisible and undemocratic way.

In some other respects however, the positions are reversed, with the European authorities being the more realistic and pragmatic. Thus, for example, most European countries do not seek to constrain the export of mass market or public domain software; nor do they constrain the exchange of cryptographic source code in electronic form. The United States in contrast goes to considerable lengths to prevent the export of anything but the weakest cryptography; moreover the US Administration makes an increasingly silly and untenable distinction between cryptographic source code on paper and in electronic form.

The reason for such differences is probably the result of the different approaches to publicity and debate in Europe and the United States. Since there is a debate in the United States authorities there have little reason to stay quiet about such matters. In contrast by avoiding public debate European groups are able to pursue their policies without having to justify them in public and there is little doubt that many of them see this as very advantageous to their cause. It is thus evident that many of these agencies are very well aware that their policies are unlikely to survive public scrutiny.

In the United States, pressure from industry has resulted in a 'fast track' export process for cryptographic systems with key length not greater than 40 bits. In practice, however, this is of little value and is widely seen by many as 'too little and too late' since 40 bit protection is simply not sufficient to provide any real protection. Indeed, over recent months several teams on the Internet has been demonstrating just how weak such keys are by mounting brute force attacks on their use within the extremely popular Netscape Navigator WEB browser. These groups used distributed computing resources across the Internet to break 40 bit keys within a few hours.

In overall terms it is evident that the exploitation of cryptography to provide security on the Internet has been severely constrained by these policies and actions. Things are now changing, however, and the end of the cold war, combined with the growing understanding of the value of cryptography, is leading to a situation where restrictions on cryptography are increasingly seen as counterproductive. In Europe, as information infrastructures grow, there will be steadily increasing pressure for a public debate like that underway in the United States and this will force the arguments out into the open. There is little doubt that this will result in changes to what are seen as increasingly outdated constraints on a now critical technology.

### 'Key Escrow' Cryptography

Faced with pressure for the wider use of cryptographic protection, the United States authorities have responded by announcing a 'Key Escrow' encryption scheme whereby the government, under legal controls, is able to gain access to the keys being used and hence the messages being exchanged.

An outline of how this might be done using the hybrid scheme discussed earlier is for each message to include a header component addressed to the government using an announced 'government public key'; the government can then use its private key to read any traffic it chooses. In practice real schemes require more than this to protect against the removal of this government access but such features can be added quite simply.

The United States administration announced a specific key escrow proposal, known as Clipper, soon after the Clinton administration came to office. The scheme, which involves the holding of cryptographic key components by two separate authorities, has received a fairly hostile reaction both inside and outside the United States. The United States appears to have sought support for this initiative from some European governments but there appears to be littler enthusiasm for the proposal, probably because of the publicity it would be certain to generate.

Commercial key escrow takes a different approach by recognising that many groups have an interest in recovering keys when problems arise. In real life people often loose keys – even cryptographic ones – and this means that they need to be able to recover their data when this happens. Moreover, people leave companies and organisations for all sorts of reasons and when they do their organisations need to be able to access the material they have been working with even if it is subject to cryptographic protection.

For these reasons, many organisations and companies need to maintain master copies of the cryptographic keys used by their employees and it is this requirement which underpins the need for Commercial Key Escrow.

Several companies and organisations have proposed such schemes and some designs have been made public so that they can be fully scrutinised to prevent allegations that there are 'backdoors' which can be exploited without seeking legal access to keys.

Very recently the United States administration has indicated its willingness to work with industry on such schemes with the possibility of unrestricted export of cryptography with keys of up to 64 bits in length.

Although it is still too soon to be certain, it looks increasingly likely that a number of Commercial Key Escrow schemes will soon be widely available.

### Cryptographic Algorithm Portability Interfaces

One possible way of promoting the wider use of cryptographic protection is to use a 'plug and play' interface so that application can be sold without cryptography which can be added later. By doing this several advantages might be gained:

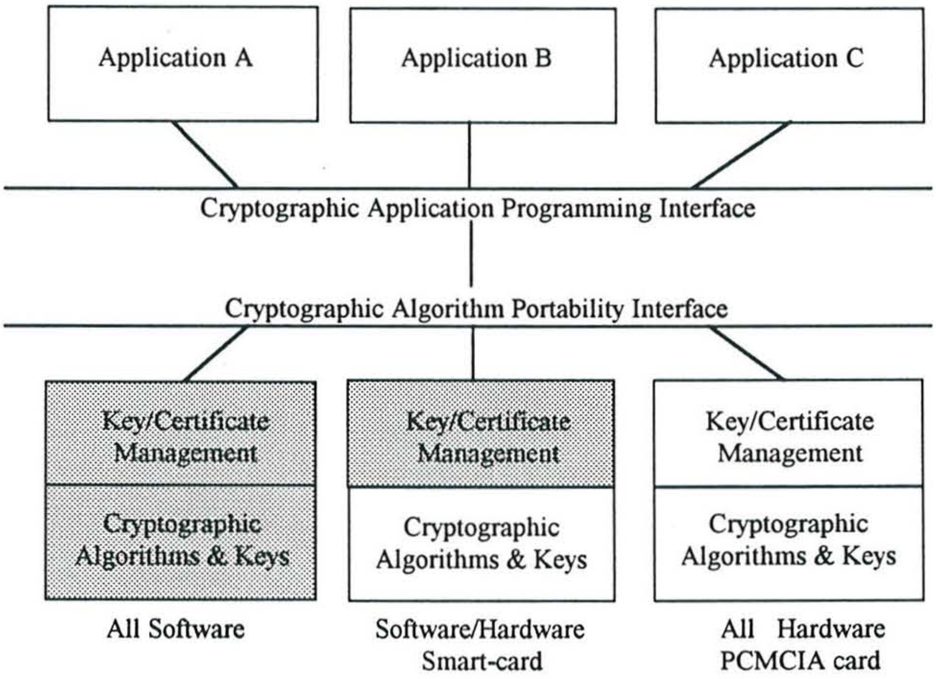
- applications can be designed without the need to worry about cryptography;
- Many different applications can exploit the same cryptographic sub-system;
- A cryptographic sub-system can support many different applications;
- governments and organisations can use whatever cryptography they wish.

These are powerful advantages and this makes it surprising that such 'plug and play' interfaces do not already exist. In practice, however, government export constraints on cryptography include not only cryptography itself but also any products specifically designed to interface to cryptography. This, of course, means that if a specific cryptographic interface is designed, it is in effect export controlled because products both 'above' and 'below' the interface are subject to export control.

Despite these problems, however, several groups are working on such interfaces. In the United States several companies have efforts in this area and the National Institute of Standards and Technology itself has a programme. In the International arena there is a group headed by Steve Walker, president of Trusted Information Systems Inc., which is seeking to select and demonstrate such 'plug and play' interfaces by proving them with a range of different cryptographic modules built in several different countries. This initiative is known as the International Cryptography Experiment (ICE). Beyond this both the Internet Engineering Task Force (IETF) and X/Open are pursuing the development of higher level cryptographic interfaces.

Although in the past national intelligence agencies have been less than enthusiastic about such interfaces, there are signs this is now changing. Staff from the US National Security Agency participated in the first ICE workshop held in December 1994 and will participate with a number of their European colleagues in the second workshop being held in The Hague later this month.

There are good reasons for optimism here since government agencies themselves want to be able to integrate their own cryptographic capabilities into standard software applications. This means that they too want such interfaces and this suggests that ideas may gain widespread support. One way in which such interfaces might be used in practice is shown in the following diagram.


Application A
Application B
Application C
Cryptographic Application Programming Interface
Cryptographic Algorithm Portability Interface
Key/Certificate Management
Cryptographic Algorithms & Keys
Key/Certificate Management
Cryptographic Algorithms & Keys
Key/Certificate Management
Cryptographic Algorithms & Keys
All Software
Software/Hardware Smart-card
All Hardware PCMCIA card

Here a common low level interface is used to support three different but interoperable products. On the left there is a low cost, low assurance 'all software' implementation. On the right there is a high cost, high assurance product in which all cryptographic functions are implemented in hardware on a PCMCIA card. Between these two alternatives a third, part software, part hardware implementation balances these pressures by using smart-card technology.

Thus the desired result of such interface developments could be to encourage a wide range of 'plug and play' cryptographic products.

## Conclusions

1996 promises to be a critical year in the evolution of an effective and affordable technology for providing privacy on the Internet and the World Wide WEB.

## DISCUSSION

**Rapporteur**: Rogério de Lemos

### Lecture One

During the talk, Dr Herbert asked what was the status of the Clipper machines. Dr Gladman answered that they were already commercially available. At this point Professor Randell made the remark that as a museum piece the Clipper machines could be compared to the Enigma cipher machine because of the number of important messages that they would have failed to protect. Dr Herbert also asked whether the commercial key escrow scheme would prevent its criminal use. Dr Gladman answered that there was no way he could stop a secret encryption. Dr Gladman went on by mentioning the case of Nixon, although he knew that he was being recorded, that did not stop him of breaking the law. He concluded by saying that there were no other mechanisms apart from commercial, and he personally would never argue for legal constraints on cryptography.

After the presentation, Professor Randell made the remark that the history of cryptography has been populated by schemes that were not as strong as one could expect.

Dr Gladman answered that the crucial thing about the commercial key escrow is that the scheme would be made public. Schemes at the moment are either secret, backed by government agencies, and criticised by the existence of back doors and trap doors, for instance, or they are public schemes that the professional agencies do not like to comment on because they can influence their market. The potential step forward is to have a fully open scheme that could be fully scrutinised by the academic community and professional agencies, with both agreeing on the strengths of the scheme, plus government endorsement; that is the step forward in the market that has been aimed to achieve with the commercial key escrow with 64 bits.

Mr Ainsworth made the comment that although a rosy picture was painted on the likely outcomes for the use of cryptography in message security, nothing was mentioned on the usage of public keys in authentication. Dr Gladman agreed with the comment by saying that during his talk he had concentrated more on confidentiality rather than authentication. He continued by saying that he believed that the existing difficulty in taking a decision towards the adoption of a particular scheme was more related to technical decisions rather than political, although there are political issues involved.

Professor Kopetz asked how secure were the systems in commercial banking. Dr Gladman replied that although he did not know the totality of the banking community, he knew that for a long time the banking community needed special licenses to use DES, and there were special licenses for the use to be international.

Professor Randell made the remark that a lot of the security and authentication mechanisms fail because they are actually inconvenient in the sense that they are not able to fit with people's abilities and inabilities. He continued by asking to what extent the usage of a whole series of commercial key escrow schemes being used for message transmission amongst independent organisations, in separate countries, will be impeded by or harmed by the human beings reactions or inabilities. Dr Gladman agreed with the remark, and answered that the problem will not be solved by the provision of national capabilities for the registration of keys because the Internet is essentially a global network, which will lead to problems of key handling and key transformation; that is why he foresaw the necessity of an international reference implementation. He also pointed out that one of the foreseen problems was how actually the certificate process of keys will be managed; he foresaw that companies will set up their own schemes.

## Lecture Two

After the talk, Dr Lesk asked what was the view of the speaker about the anonymous re-mailers. Dr Gladman replied that he could see real difficulties in dealing with the problem. He also said that he did not see imposed legislation as a solution, he would rather prefer to see the community on the Internet to legislate by itself, in a form of agreement, to regulate the use of this sort of service.

Professor O'Riordan asked who in the speaker's opinion was going to pay for the browsing over the net. Dr Gladman answered that he personally did it on his own expenses, he also said that in his opinion the community in general is paying the expenses by becoming a member of Microsoft network, for example. He also admitted the existence of a lot of altruism, mainly concerned with university hosts, however he did not know how the situation will evolve in the future. Still on this topic, Professor Randell made a comment about the North of England network initiative whose attempt, because of the importance of information, is to have a levelled playing field to avoid the great danger of having "information haves and have nots". In his opinion, this concern has been much more understood at the level of Brussels than at the level of London, or perhaps any other capital in Europe, in the sense that there has been a lot of effort and money from Brussels trying to even the playing field.

Professor Whitfield raised the issue of standards by mentioning that in his opinion in the 80's governments, and the European Commission as well, have tried to use standardisation as a mechanism to obtain competitive advantage, such as the standards involving television, which is different from the Internet process.

Dr Gladman replied that in his opinion there have been two domains of standardisation, one that has viewed standardisation as a competitive advantage, and the other that says if one should follow the market growth, outstripping the process of competitive advantage for the benefit of everyone, being a good example of this view are the recent audio standards; people start to realise that a standard is a market growth form and it is better to have one standard than two or three in fighting for the market.

Professor Katzenelson made the remark that the speaker has not offered any remedy for the politicians lagging behind of the state of the art. Dr Gladman admitted that he did have not any solution. In some respect, he personally would like to see some action, but on the other hand, the Internet has been evolving quite well without any intervention, why should we then worry about the dangers of an ignorant intervention that can be worse than no intervention at all. In his opinion, let the things keep on moving so fast that by the time that the people start thinking about legislation it becomes too late. The problem is that politicians start panicking because this is power to the people and power away from the politicians, and actually most politicians do not really believe in power to the people, they believe in power for the politicians, so that is why we can expect politicians not to like the Internet.