Markus Kuhn
Schlehenweg 9
D-91080 Uttenreuth
Germany

phone/fax: +49 9131 52226

electronic mail:
mskuhn@cip.informatik.uni-erlangen.de

1996-05-23

· Markus Kuhn · Schlehenweg 9 · D-91080 Uttenreuth ·

European Commission
Mr. Mario Monti
200 rue de la Loi
B-1049 Brussels
Belgium

your date your reference

Comment on the Commission Green Paper "Legal Protection for Encrypted Services in the Internal Market – Consultation on the Need for Community Action" published 1996-03-06

Dear Mr. Monti!

With great interest I have read the Commission's *Green Paper* on the suggested legal harmonization with regard to pay-TV piracy in the European Union. As this document invites any person to participate in the open consultations, I would like to send you with this letter my comments about various issues discussed in the *Green Paper*. I believe that my comments provide a view on the need for special laws against unauthorized pay-TV reception that deserve serious consideration.

Please let me first briefly introduce myself. I am a 25-year old German computer science student very close to graduation and I am specializing in computer security and the use of encrypted services in the Information Society. I plan to pursue a career in the now rapidly emerging European industry dealing with computer security, encryption, and access control. This explains my strong interest in the *Green Paper* as a prospective member of the access control device industry.

I have also spent during the past two years considerable time with analyzing existing pay-TV access control systems for personal reasons. My previous work includes the implementation of a software for real-time image reconstruction of the *BSkyB* broadcasts on Astra by reversing the active-line-rotation encryption mathematically, the implementation of an MS-DOS personal computer software ("*Season7*") that allows to replace a *BSkyB* smart card by a PC with a simple cheap smart card connector adapter cable, and the implementation of an MS-DOS PC software ("*Phoenix*") that allowed to reenable expired

BSkyB smart cards. I have never participated in commercial pay-TV piracy and I have shared all my technical findings and decryption software freely available over the Internet with other interested persons, mostly other students at technical universities. However, I have been in informal contact with several commercial pay-TV piracy device and access control system manufacturers and I believe that I have very good insight into the community concerned with pay-TV access control.

The main reason for me to purchase satellite-TV reception equipment was the desire to get access to non-German language programs, especially from UK and F. I was very frustrated when around 2.5 years ago, *BSkyB* started to scramble all their programs and did not provide any legal way for Germans to subscribe to their service. My successes in developing unauthorized technical means for the *BSkyB* decryption were the only way for me to get continued access to English language TV channels. This explains my strong interest in the *Green Paper* as a frustrated customer on the European pay-TV market.

I would like to comment on the following statements made in the *Green Paper*:

1) Estimated Number of Unauthorized Decoding Devices

The estimated number of present unauthorized decoding devices is given as "5 to 20% of the total number of decoding devices in circulation" (page 5). Unfortunately, no source for this information is given. This number is in my opinion very misleading. Although the 5% number might be a realistic upper limit for the number of unauthorized devices that have ever been produced in Europe, the relevant figure for an estimation of the market share is the number of devices that are still operational currently.

The pay-TV providers regularly exchange encryption codes. Many providers implement frequent simple counter measures that render existing pirate devices ineffective; *BSkyB*'s technicians for example have developed sophisticated techniques that allow easy and effective counter measures against unauthorized devices every few days. In addition, subscription cards are exchanged every few years. Pirate device manufacturers are often not able to provide updates against counter measures, updates require several days or even weeks, and many updates are only available by purchasing a new device instead of upgrading the old hardware. This has caused considerable frustration among consumers of pirate devices. A large number of consumers which have once bought one or often several pirate devices has found out that these devices are not operational or upgradeable any more and they have now returned to the official subscription where possible or they have given up access to the channel entirely.

A realistic estimation is that **less then one tenth of the unauthorized decoding devices that have been produced are still operational, while most of the official devices are still in full use**. This would correct the **effective market share** of unauthorized devices down to **less than 0.5%** of the total number of decoding devices in circulation. In addition, the Commission should consider that almost all customers of unauthorized decoding devices learn about these devices from the satellite TV press and are well informed about the risks and frequent counter measures. At least in D, the largest number of distributed pirate devices decoded the UK *BSkyB* channels, for which **legal access to the service is completely unavailable** in D. Considering the frustration caused by frequent electronic counter measures, most users of unauthorized decoding devices for

BSkyB in D (probably the largest European pirate market segment) would have prefered an official subscription if it had been available.

2) Image of the European Access Control Device Industry

In section 3.2, the *Green Paper* mentions the "loss of income and credibility for the suppliers of the technology" as one of the negative consequences of access control piracy. The argument is that operators looking for the most secure available encryption system will not select one which has a history of successful unofficial access.

I was seriously surprised to find such an obvious example of inverse logic in an otherwise well-written report. The opposite of the above statement is true. **The security of an access control system can only be fully estimated and improved by encouraging skilled persons to attack it.** If a system has not been compromised by pirates, because potential pirates were discouraged from the effort by strict legislation that makes any such attempt illegal, potential customers have no reliable way of determining the security of the system. **If an access control system has not been compromised by pirates, although any attempt to produce unauthorized devices would have been legal and financially attractive, this is the only real proof for the quality of the security system.** Security studies performed by a few experts paid by the manufacturer or customer for evaluating a system have not nearly the innovative potential to find hidden weaknesses in an access control system design that the effort of skilled and highly motivated people from all over Europe provides.

Enforcing strict legal regulations against pay-TV pirates would render Europe useless as a demonstration market for the export of access control and other vital Information Society technologies. Customers of access control systems will certainly prefer to buy highly secure systems from manufacturers that have survived the fight against piracy by advanced technical means instead of legal protectionism and that have a long history of experience with counter measures against unofficial piracy devices.

In case pay-TV piracy will become one day effectively banned by strict new laws against unauthorized devices, the European access control system industry will quickly get a bad reputation on the world market as an industry that has lost the technical competition with pay-TV piracy and has in its technical weakness searched protection under comfortable legislation.

The Commission should consider that **considerable advances in access control security technology** compared to the simple early systems *VideoCrypt*, *Syster*, and *EuroCrypt* that are used today is possible. Significant new developments will leave the laboratories of manufacturers in the next few months and years. Just to name one minor example, the paper [A. Fiat, M. Naor: Broadcast Encryption, CRYPTO 93 Proceedings, pp. 480–491] demonstrates a brand new easy to use encryption technology, that puts several different secrets in each smart card, such that no two distributed smart cards contain identical secrets. If pirates manage to analyze with great effort a few single smart cards and copy the secrets found there into their unauthorized devices, the broadcaster will only have to exchange a minor fraction of less than one percent of all official smartcards before the encryption can be changed quickly and the system will be completely secure again. Once this new technology is implemented, pay-TV pirates will have to analyze the secrets of many thousand smart cards in order to enforce a complete exchange of all official cards. All this

can be implemented with the cost and performance restrictions of technology available today.

This is just one single example of new technology that is currently in development and will help to make access control systems considerably more secure against even very well equipped and knowledgeable pirates. **Such new security technology would certainly not have been developed as quickly without the existing pay-TV piracy market.** The competition with pay-TV pirates has enforced the European pay-TV industry to develop many new highly innovative security technologies.

Many of the basic technologies used in pay-TV access control systems like very cheap tamper-proof smart card microprocessors, highly analysis-resistant customer specific circuitry, cryptographic security protocols and algorithms, and innovative security key management techniques can not only be applied to build more secure pay-TV access control systems. They are **important building blocks for secure system designs for many new multimedia systems in the Information Society**.

We are facing a number of new applications of encryption like digital cash and teleshopping, where the potential damage caused by security deficiencies in access control mechanisms can do **significantly more harm than in the pay-TV industry**. In these future Information Society systems, security deficiencies could allow criminal activity against individual EU citizens involving significant personal financial loss. Security problems in digital cash systems can even cause unexpected inflation of the new European currency if criminals find a way to fake digital money and insert new currency value into the system; the economic and political consequences of such criminal activity are significant.

The current efforts of the European pay-TV industry to find cheap and effective technical means of protecting encrypted information will give the European industry in the near future a **significant advantage over other manufacturers active in markets where pay-TV piracy is controlled by legal means**. The competition with pay-TV pirates enforces access control manufacturers and the semiconductor industry to stay technologically at the leading edge of development. The lack of legal protection and the expected technical successes against piracy will give the European access control and computer security industry an **excellent international reputation** and a corresponding international **market success in a key technology of the next two decades**. The very limited economic damage that pay-TV piracy can inflict compared to criminal activity against other Information Society encryption services like digital money or GSM, which are based on the same security technology, makes the pay-TV market an excellent preparatory stage in which the European industry can find **cost-effective technical solutions against the dangers of the forthcoming Information Society**.

I have done myself promising research in my diploma thesis about security systems, and I would only be proud of a lack of piracy against my improved system if I could demonstrate the security of my ideas on an open market with no strong legal threat against potential motivated pirates. There exist possible technical solutions to the pay-TV piracy problem that have the potential to make legal protection of service providers unnecessary.

3) Prohibition of Manufacturing, Possession, and Use for Private Purposes

On page 39–40, the *Green Paper* suggests that the manufacture and the possession of unauthorized decryption devices for private use as well as any decoding of encrypted broadcasts

could be prohibited by the required harmonized regulation for pay-TV access control. The *Green Paper* also suggests "deterrent penalties for the breach of these provisions".

The suggested prohibited activities include any manufacturing, possession, and use of unauthorized decoding devices, even if all these activities have only been performed for private purposes. I strongly feel that this is unjustified and would like to explain the reason for this view, which might not be completely obvious for a less technically interested person. Please let me therefore describe in some detail, what exactly it means to manufacture and possess one of these devices:

As stated in the introduction, I have myself developed a number of "unauthorized decryption devices" just for personal and educational purposes, without any intent to harm a broadcaster or anyone else. One of these decryption devices consists of a simple adapter cable that allowed me to connect the serial port of by personal computer to the smart card connector of a normal *VideoCrypt* decoder. The design of this device was quite obvious and based on information found in any introductory electronics text book. The basic components (cable, connector, two standard chips, five capacitors, printed circuit board) costed around 11 Ecu and I bought them from a small local electronics shop. In addition, I spent around 20 hours writing a special software for my personal computer. This software, my normal personal computer, and the simple adapter cable allowed me to watch all *BSkyB* channels over several months. The adapter cable I manufactured can not necessarily be seen as a device only suitable for pay-TV piracy. In effect, it is a universal adapter between the computer industry standards EIA-232-E (PC serial port) and ISO 7816 (smart card connector). It can be used for various test, demonstration, and diagnosis purposes on any smartcard system. This simple adapter can hardly be any more illegal than any other common piece of computer equipment like a printer cable, however it is a device that can be used for unauthorized decryption of pay-TV services among many other uses.

Although the following is just a naïve common sense argument, I hope you can understand my serious concern: **I consider it completely unjustified that developing, constructing, possessing, and testing my software and my adapter cable on a normal VideoCrypt decoder as part of my private activities as a very curious computer science student and hobby electronics fan might one day constitute a criminal action that could be prosecuted with up to two or three years of prison.** After all, the images which I made visible on my TV screen were commonly available signals that have been broadcasted directly to my home. I did not "steal" them from anywhere, and I deeply feel that the European Union has no moral right to forbid me to process received broadcast radio signals in my house in any way I want with self developed software, including making them visible on a screen. **Considering my personal interest in electronics experiments and computer security, I would consider any new law forbidding the private manufacture of decoding devices an unjustified restriction of my personal freedom.**

In another project, I did not even use a *VideoCrypt* decoder or any other pay-TV related device at all. I loaded the encrypted TV images with a normal video signal processing device into a university computer and sent the image data through a special software that I had originally developed for a medical data processing project, but that was easily modified such that it would reverse the active-line-rotation scrambling of *VideoCrypt*. Together with a friend, I implemented this software on a supercomputer of the University of Erlangen and this way, I was able to decode encrypted *BSkyB* channels and watch a few minutes of

a science-fiction series on our university computer screen. I only applied a mathematical algorithm to the received signal with a very fast computer. This small project was only intended as an impressive demonstration of the capabilities of a new multimedia real-time video processing system that had been developed at that time at the University of Erlangen. However, my software effectively turned the university supercomputer into a "unauthorized decoding device" and with the new legislation proposed in the *Green Paper*, the University of Erlangen could in the future be legally prosecuted for possession of an unauthorized decoding device in the form of a fast computer suitable for video signal processing. This hardly seems justified to me.

I am very concerned by the idea that these interesting experiments and those performed by a few other people with similar skills and interests who I know from discussions on the Internet might one day be illegal crimes under a new European law. **Is it really important for the Commission to make private educational experiments with signals received at home illegal?**

In addition, I would like to point out that almost all unauthorized decryption devices are simple printed circuit boards that contain only a cheap general purpose microprocessor available in any better electronics shop in most cities for around 9 Ecu. These devices could be used for a large number of purposes like door access control systems, personal cryptographic modules for e-mail and hard disk encryption, industrial data logging, etc. A friend of mine has used a device originally produced as an unauthorized pay-TV smart card replacement in his diploma thesis project, where it was an important component of an authentication system for computer networks. Nothing on these devices is characteristic for their usability as unauthorized decryption devices. **Only the software loaded into the general purpose microprocessor makes the device useful for decrypting pay-TV services.** It is impossible to proof that a simple commonly available microprocessor fixed on a piece of plastic with ISO 7816 smart card contacts has anything to do with a pay-TV access control system, because of the many other uses of such devices. The software in the microprocessor could be protected by special access codes like a secret number without which the decryption can not be started, and the software could be transmitted easily via modem or on international computer networks like the Internet in encrypted form from one user to the next. All this can be used very easily in such a way that a **proof of possession of software suitable for unauthorized access of a pay-TV service will become virtually impossible**.

It might make sense to provide some limited new legislation against the marketing and distribution of pay-TV piracy software contained in suitable devices for commercial purposes in order to protect inexperienced customers from believing that they have obtained an official subscription instead of an unauthorized device. But anything beyond this will be extremely difficult to proof and should therefore not be made illegal. Without the ability to advertise and distribute piracy equipment for commercial purposes, the large scale use of such devices will become quickly limited to only a small harmless grey market and to a small number of skilled hobby electronic freaks who can build and use these devices privately. This will certainly not do any harm to the service operators, and therefore **any community action towards a ban of private manufacture, possession, and use of these devices is in my opinion unjustified**.

The Commission should also consider seriously the dangers of providing new ways for broadcasters to bring a claim for damages and interest. Such a new legal means could

be abused by broadcasters to threat a harmless hobby electronics developer of unauthorized access devices or a journalist, who only shared technical knowledge with others on public channels like computer magazines or the Internet. It will be extremely difficult if not impossible to get any reasonable figures about possible real financial damage for a broadcaster, and it is not unlikely that broadcasters with clever lawyers can convince courts with huge phantasy numbers like the "20%" value mentioned in the introduction of the *Green Paper*.

Conclusion

The *Green Paper* is in large parts an excellent description of the current situation of the pay-TV industry in Europe. However, some very important arguments and conclusions for suggested community action seem to have been heavily influenced by the view of the service operators. This is no surprise considering the intensive lobbyistic efforts of a pressure group formed by the broadcasters represented in the DVB consortium.

Although I am only a single technically experienced individual without any budget or legal assistance, I hope that I have been able to offer you a new view on some of the arguments that have been brought to the Commission by the broadcasters.

- First, I consider the figures and arguments about damage caused by pay-TV piracy so far and in the future unrealistic and if not greatly exaggerated then at least presented with an interpretation strongly biased towards the interests of the broadcasters.
- Second, it is my impression that the authors of the *Green Paper* greatly underestimate the potential of innovative new developments in the access control industry that will allow to build new systems or upgrade existing systems with considerably more secure smartcards. **The description of the state of the art in access control in the Green Paper is limited to the situation around 1987 when VideoCrypt and EuroCrypt have been developed.** New cryptographic concepts as well as advances in the design of security hardware have a great potential in providing very **cost effective secure technical solutions** that will render legislation intended to protect the broadcasters unnecessary.
- The battle against pay-TV piracy has already initiated a number of **important innovations** in the access control and microelectronics industry and many more are to be expected in the near future. The race against skilled competitors will enforce the security hardware industry to stay highly innovative and to come up with a large variety of cost effective better solutions. This way, a **liberal legislation with regard to unauthorized access to pay-TV systems will speed-up the development of cheap computer security building blocks suitable for the mass market**. The U.S. industry is perhaps currently the world leader in the major computer security markets, but these are so far markets of military and commercial users with very **different requirements** compared to the mass market requirements of pay-TV access control technology. Availability of **enabling technology for mass market security design** will be an important factor in the run-up for the Information Society.
- Fourth, even if the previous argument should not convince the Commission, I see no good reason for taking any steps against the manufacture, possession, and use of unauthorized decryption devices for **purely non-commercial private purposes**. This will criminalize **harmless experimental efforts** of a small number of hobby

electronics fans like myself, that can impossibly cause any measurable financial damage to service providers. In addition, a liberal view on the manufacture and possession of these devices will avoid **interpretation problems** of these new regulations considering the many **alternative uses of exactly the same hardware**.

– Fifth, to the best of my knowledge, the majority of piracy equipment has been sold to customers in **countries where a legal subscription to the pirated service was not available**. Because of the effective counter measures, long pirate device update times, and frequent smartcard exchanges, pirate devices are usually not highly attractive for customers that can subscribe to the official service.

  A pan-European television market in which **all Europeans** can subscribe to **all channels** available on the satellites which they receive is one important step towards **an aspect of European unity and identity that will be present in the every-day lives of many EU citizens**. The availability of many pan-European TV channels will also help to **break down the language barriers**, one of Europe's largest problems in the competition with other unified markets like North America. **The Commission should not encourage broadcasters like BSkyB to limit their service to small parts of Europe by making access in other parts of Europe illegal for citizens seeking foreign language TV services.** Especially this argument, which has already been discussed often in the trade press and in on-line discussion forums and therefore seems to be an important issue to many satellite dish owners in the EU, has been completely ignored in the *Green Paper*. Please include this wish for cultural diversity of many citizens and their desire for a pan-European satellite channel market into the argumentation, which has so far been dominated by the view of broadcasters and their **minor license policy problems**.

  The idea of a European Union appears of little value to a satellite dish owner who finds out that she can not receive the same TV channels in D or I as in F or UK. The idea of a European Union appears even more strange to the average satellite dish owner if the Commission of this Union makes alternative unauthorized ways to access these channels illegal!

Considering these arguments from the point of view of a service customer or someone interested in the positive **long-term development of the European computer security technology industry**, there appears to be no hurry to follow the regulation suggestions of the broadcasters and only the following Community actions seem to be advisable to me:

– Harmonize the various national pay-TV laws towards a **very liberal position** with regard to unauthorized access of service, especially in regions where no official way of subscribing the service is possible. This will encourage the free movement of services and keep the security technology market interesting. Only commercial advertising of piracy equipment should be prohibited in order to protect inexperienced consumers and limit the potential market share of unauthorized access devices seriously. This will require in many countries only very minor changes in existing regulations.

– Interested parties should not be enabled especially to bring a claim for damages and interest, as the damage caused by unauthorized access devices is **practically not quantifiable**.

– Under no circumstances should the construction, possession, and use of unauthorized access control devices or software for **non-commercial private purposes** be made

illegal. This will protect inexperienced consumers and harmless hobby electronic activists interested in the subject against unjustified and unnecessary legal action.

The currently proposed regulation in the *Green Paper* reads like a wish list of the broadcaster lobby. It is my hope that this letter has contributed to the efforts of the Commission to get an unbiased view of all involved sides on the matter of encrypted TV services. I also hope that the Commission will be able to make a decision that is not only based on the very specific view of the broadcasters and their DVB pressure group, but that takes the individual citizens' interests as well into account as the negative effects on the industry caused by a too comfortable strict legal protection from problems that can much more effectively be controlled by innovative technology required by the global markets of the future Information Society.

Sincerely yours,

Markus Kuhn