Markus G. Kuhn
University of Cambridge
Computer Laboratory
New Museums Site, Pembroke St
Cambridge CB2 3QG
United Kingdom

phone: +44 1223 3-34676
fax: +44 1223 3-34678

email: Markus.Kuhn@cl.cam.ac.uk
url: http://www.cl.cam.ac.uk/~mgk25/
pgp: F0 49 0D 10 F0 FA F6 5B
E7 BC 78 54 5F 6E 46 2E

1998-03-20

· MG Kuhn · Computer Lab · Cambridge CB2 3QG · UK ·

To the members of the
European Parliament
Committee on Legal Affairs
and Citizens' Rights

your date your reference

Conditional Access Draft Directive COM(97)365 as amended by the Anastassopoulos report

Dear Sir,

I would like to express my concerns about the "Proposal for a European Parliament and Council Directive on the Legal Protection of Services based on, or consisting of, Conditional Access" (COM(97)365) and especially about the amendments to this directive proposed in the report by Mr. Georgios Anastassopoulos dated 1998-02-09. I am an academic researcher with expertise in encryption techniques and conditional-access systems and I represent only myself as a German citizen. I have already presented my concerns in my letter dated 1996-05-23 to Commissioner Mario Monti after the publication of the European Commission Green Paper "Legal Protection for Encrypted Services in the Internal Market" published 1996-03-06. This earlier letter as well as additional material on this topic is available publicly on my Internet page <http://www.cl.cam.ac.uk/~mgk25/ca-law/>.

As you certainly know, the deregulation of television monopolies has enabled private broadcasters to offer subscription based pay-TV programmes. To ensure their revenue, they encrypt the broadcast signals and provide decoders only to subscribers who pay a certain fee. The security of these decoders has in the past few years been compromised by hackers and unauthorized decoders have become available on the market. Fearing the cost of having to invest in the development of more secure encryption techniques and decoders, the broadcasters started an intensive lobbying effort to introduce new legislation. The broadcasters request very strong legal protection that would render any activity related to the unauthorized decryption of their programmes illegal and punishable.

As might be expected from the intensive lobbying that led to draft directive COM(97)356 and the Anastassopoulos amendments, the aspects of the situation have been presented in a rather biased way by the pay-TV broadcasters. I would like to present the other side of the case and urge you to reject this proposed directive.

• Modern encryption technology allows manufacturers to design conditional-access systems that provide a more than sufficiently strong technological protection against unauthorized

access. It is therefore justified to leave it in the responsibility of the service providers to protect their services with technical means and it is not necessary to protect their profit with legislation. The cost of replacing the currently fielded insufficiently secure decoders is negligible, since all these decoders have to be replaced anyway for the migration to digital TV broadcasting in the next four years.

• Even though it is true that the first generation of conditional-access systems that was developed in the 1980s showed weaknesses that allowed some very limited degree of piracy to take place, more recent innovative developments will lead to extremely high levels of protection for pay-TV and pay-radio broadcasts making additional legislation unnecessary. Examples for such recent technological progresses are the replacement of the currently used medium-security EEPROM smartcard technology by more modern low-cost high-security processor modules that are based on battery-buffered SRAM technology (such as the DalSemi DS1954, to name just one already existing product). The "Broadcast Encryption" scheme described in 1993 by Amos Fiat and Moni Naor from the Weizman Institute in Israel and other new cryptographic techniques prevent a hacker who reverse-engineers a single decoder compromising the entire system with the information gained from it.

• The same protection technology (cryptography, smartcards, etc.) that is applied in pay-TV conditional-access systems is also used in other forthcoming Information Society applications including digital signatures, electronic commerce, electronic cash, secure communication, and digital voting. Compared to the risk of some minor temporary pay-TV piracy, the failure of technical security in these systems would be much more dangerous to the financial and legal situation of individuals and organizations. Pay-TV conditional-access systems are therefore an important large-scale demonstration step for the security of modern digital protection technology. If the industry does not manage to protect a relatively simple system like pay-TV conditional access, then we will face far greater risks for society with fraud on other applications that use essentially the very same technologies and that have to be implemented with comparable cost restrictions.

• The figure of 200 million ECU annual loss caused by unauthorized pay-TV decryption in Europe presented by the industry to the European Commission is an extremely crude and biased estimate. The number is possibly one order of magnitude too high. Conditional-access system operators like BSkyB and NDS claim that their system is currently completely uncompromised and has never suffered more than 5% of piracy; in recent court cases, they have put losses at £30m for the whole period 1986–1998.

• A lack of strong legal protection of conditional-access systems will motivate the industry to develop appropriate technical protection, from which the Information Society will then profit in later more critical applications. The legal protection that you are about to vote on defines the selective pressure on security technologies. Less legal protection means more selective pressure, which leads to a faster technological evolution.

The best approach would be not to introduce new legislation for the legal protection of pay-TV broadcasters at all. They have been given the privilege to use a part of the radio spectrum—a very limited and precious resource—for their commercial interests in a way that excludes the majority of television set owners from any benefit. They should be satisfied with that privilege and should be responsible for ensuring their revenue by technical means; they should not make it the task of the legislator to fix the flaws in their current technology for them.

It is even more worrying that the proposed amendments in the Anastassopoulos Report extend the legal protection of pay-TV broadcasters far beyond the original draft directive, to make it prohibit not only the commercial sale of unauthorized decryption devices. By adding the open formulation "for direct or indirect financial gain" to the previously used term "for commercial purposes", the amendment tries to target the directive against private consumers as well. The Anastassopoulos Report essentially proposes to criminalize the private possession and use of unauthorized decryption devices.

Worst of all, the Anastassopoulos Report even lists as infringing activities "the advertising and provision of information concerning activities and measures facilitating unauthorized access", which would criminalize even the private or scientific discussion of the technology of conditional-access systems if the presented information could in any way assist anyone in decrypting pay-TV signals. I am especially concerned about this part of the proposal, because I have myself conducted numerous decryption experiments to demonstrate security weaknesses of conditional-access systems several years ago and I have published the results. My diploma thesis as well as two of my scientific papers and the talks that I have given at various universities, conferences and to a group of German Telekom engineers would all have been illegal activities if the regulations suggested by the amended conditional-access directive had already been in place. This is a very frightening prospect for my freedom of speech as an academic researcher and it clearly demonstrates how out of proportion the conditional-access directive has become.

The authors of the draft directive and the Green Paper claim that the directive is necessary to ensure the free movement of services in the common market. However, the pay-TV broadcasters have not at all been interested in the free movement of services. The content providers, especially the major Hollywood studios, try to avoid pan-European TV broadcasts. Their marketing strategy has always been to sell broadcasting rights separately to small geographic regions, because this helps them to maximize their profit through regional exclusive licensing contracts and to control the markets better this way.

One example: I purchased in 1993 in Germany a satellite TV receiver to watch British programmes to improve my proficiency in English. Two months later, almost all British channels were encrypted. I tried to get an official subscription for these channels, but I was informed, very much in contrast to the idea of a free movement of services, that British Sky Broadcasting is only selling subscriptions in Great Britain and Ireland and not in the rest of Europe, although the signal can be received all over the EU.

Europe-wide satellite television could help in breaking down language barriers. Conditional access is the technology used to restrict satellite broadcasting services artificially to small regions, although the signal can be received everywhere. Free movement of service is not the issue for the broadcasters; they use conditional access first of all for regional market segmentation. Under that perspective, the conditional-access directive is hardly something that earns the support of the European Parliament.

Yours sincerely,

Markus Kuhn