4 Palmers Green
St Johns
Dr Brian Gladman
Worcester WR2 4JY
gladman@seven77.demon.co.uk
+44 1905 740902

15th March 1998

Open Letter to:

Mr John Corrie, MEP
98 High Street
Evesham
United Kingdom WR11 4HE

Dear Mr Corrie,

Proposal for a European Parliament and Council Directive on the Legal Protection of Services based on, or consisting of, Conditional Access

I am writing to seek your support in preventing some unreasonable and potentially damaging draft provisions being adopted as elements within the Directive referenced above.

In outline the original aim of this Directive was to make it illegal to commercially manufacture or sell products that allow access to fee-based information services without payment of the associated fees. The main activity envisaged here is pay-TV but the principle is expected to apply to any information services involving access fees.

Although the original proposal is sensible it now seems that lobby groups for the pay-TV industry are seeking amendments that will go much further. In particular a proposal known as the *Anastassopoulos Report* (published on the 9th February 1998) seeks changes that are unworkable, potentially very damaging and highly counterproductive.

In outline, the proposed amendments to the original draft seek to make it illegal to:

- own the means for unauthorised access to conditional access services;
- to provide information that could facilitate unauthorised access.

Although these extensions might seem to be plausible at first sight, it turns out that each of them could turn the completely innocent activities of law-abiding citizens into criminal acts. Worse than this the second amendment would make the discussion and teaching of virtually all information security techniques unlawful.

Ownership of the Means for Unauthorised Access

Although the draft provides for national discretion in making the ownership of unauthorised access devices illegal, it seeks to promote such measures and hence encourages action leading to a number of dangers that would be better avoided.

The first difficulty is that any personal computer equipped with appropriate TV reception capabilities would be illegal under such provisions. For example, I own just such a computer system and, although I do not use it for unauthorised access, it could in principle be used in this way. Although it might be argued that I need special software for this purpose, in practice it will be impossible for me to guarantee that the software that I have does not provide for this in some way that I am unaware of. As a result this proposal could turn me into a criminal even though I have absolutely no intent to use my system for any criminal purpose.

Secondly, making the possession of unauthorised access devices illegal could turn many innocent and entirely law-abiding citizens into criminals. Although, no doubt some owners of illegal devices are knowingly using them, it seems likely that many are unaware of this. In all probability a number of users have bought them in good faith without realising that they provide access in an unlawful manner. Such consumers are as much the victims of those who sell these devices as the broadcasters themselves and it is quite wrong in my view to seek to turn them into criminals.

For these reasons I consider it essential that the focus of any legislation should be to protect service providers and consumers from those who ***manufacture or sell*** illegal access devices. Making possession illegal is unworkable and simply risks turning many honest and law-abiding citizens into criminals.

Providing Information that can Facilitate Unauthorised Access

Providing conditional access involves a battle between service providers, who wish to protect their information, and those who wish to unlawfully offer access to it. At first sight it might seem sensible to try and prevent the open discussion of the means for unlawful access but when this is considered more carefully it turns out that this will not only be unworkable but will, in fact, have exactly the opposite effect to that intended.

In the field of information security there is a continuous tension between the need to share information in order to improve the design of systems and the risk that such sharing will help those who are intent on breaking into the systems concerned.

The first reaction to this tension – 'security through obscurity' – is to attempt to hide designs and to prevent discussion of them so that information is denied to those who might try to break into them. The second reaction is to openly publish design details so that the expert community as a whole can consider the approach being adopted and hence identify potential weaknesses.

The overwhelming consensus within the professional information security community is that the open discussion approach leads to better security.

The fact is that open discussion of the means for information protection also requires an equally open discussion of the ways in which systems can be attacked. Without understanding how attacks can be mounted it is simply not possible to plan an effective defence. Without such discussion the field of information security would not advance and we would be left with systems that could be easily exploited by almost anyone.

Although open discussion involves a risk that some will misuse the knowledge gained, more importantly it allows a much wider community to become involved. Because a large majority of those involved will use the resulting knowledge honestly the overall result for the community as a whole is strongly positive.

In contrast when open discussion is banned, system flaws are not discovered quickly and they remain present in systems for long periods. The ban on open discussion does not prevent those with unlawful intentions from exchanging information – it simply drives them underground. Meanwhile law-abiding citizens are unable to discuss or teach information security techniques with the result that the security performance of systems remains poor. Worse still, the ban means that society cannot train the skilled information security professionals on which its future safety and security will depend.

Thus, far from reducing the ability of those who offer illegal access, a ban on discussion will actually have precisely the opposite effect – such a measure would allow these people to continue their illicit activities without fear of being undermined by the progressive security enhancements that open discussion will foster.

Conclusion

In my view the original intention of this Directive – to make it illegal to commercially manufacture or sell illegal access devices – was sensible. Such a measure would protect service providers and their honest customers without creating difficulties for others.

But the amendments suggested in the *Anastassopoulos Report* would convert a carefully targeted proposal into one that would be unworkable. It would be completely unenforceable and would carry the serious risk of converting honest, law-abiding citizens into criminals. Worse still, it would undermine the ability of the information security community to share the information needed to improve systems and the ability of society to develop the knowledge and skills needed to make the future information systems on which we will all depend safe and secure.

In summary these proposed changes to the original draft Directive are ill-conceived; they can only be seen as an attempt by an overzealous community to overcome its own shortcomings by imposing unreasonable, unworkable and damaging provisions on the rest of society.

I urge you to use your influence to ensure that these proposals are rejected.

Yours sincerely,

Dr Brian Gladman