Ian White, MEP
138 Gloucester Road
North Filton,
BRISTOL
BS12 7BQ

11 Oakwood Road
Henleaze
BRISTOL
BS9 4NP

tel. 0117 922 8071 (work)
tel. 0117 962 4408 (home)
stefek_zaba@hplb.hp.co.uk

13 March 1998

Dear Ian,

Draft EU directive would ban research on security systems

Introduction: "Anti-piracy" directive being drafted

I'm writing as a constituent of yours to alert you to a technical issue which has impact on the economic activity of the UK, including Bristol, and on academic freedom. The issue concerns a proposed EU Directive, currently at an early stage of preparation, whose main aim is — unobjectionably — to make illegal the activities of those who gain commercially from the "pirating" of scrambled TV signals such as satellite TV broadcasts. However, a recently proposed amendment to the draft Directive would mandate member states to criminalise the "... provision of information concerning activities and measures facilitating unauthorized access" (page 8, Amendment 12, c2 of the Draft Report COM(97)0356 - C4-0475/97).

Broad Ban is Self-Defeating

This extremely broad ban on discussing, investigating, and demonstrating the weaknesses of actual or proposed scrambling or authorisation systems would stifle the very research which makes these and related systems — such as the UK Government.Direct initiative — fit for their intended purpose. Suppressing such research, whether in industry — such as the secure systems research group I work in at Hewlett-Packard, or in academia, such as work on security at UWE and at Bristol University — would be short-sighted in its consequences even for the interests this Directive is intended to protect; it would be entirely inimical to the broader interests of secure access to public networks such as the Internet towards which the UK is moving, and in whose evolution the Bristol region plays a modest but not insignificant part.

Not Only Conditional-Access TV Affected

Though initially motivated by satellite TV anti-piracy interests, the Directive is drafted to include in its scope "Information Society services within the meaning of Article 1 2 of Council Directive 83/189/EEC as amended", which cover any kind of

personalised on-line transaction. A DG XV commentary defines those "Information Society services" as being

> all existing or new types of services that will be provided at a distance, by electronic means and on the individualised request of a service receiver. This definition of "service" would cover, for example, on-line professional services (e.g. solicitors, estate agents, stockbrokers, insurance, health care, travel agents), interactive entertainment (e.g. video on demand, on-line video-games, virtual visits to museums), on-line information (e.g. electronic libraries and newspapers, financial information), virtual shopping malls and distance learning services.

Progress in Information Security Achieved By Open Review

It is well-established practice in the field of commercial and academic development of secure systems that both general principles and particular implementations are subjected to open scrutiny. The field makes progress by fierce cross-examination of proposed new approaches in both theory and practice. In our work at HP Laboratories Bristol, my colleagues and I have frequent cause to examine both published proposals for secured systems and actual implemented systems, to see if they meet their stated criteria. Often they do not: I myself have demonstrated to a major UK financial institution problems with their system as deployed, going on to advise them how to correct the demonstrated flaw; and worked with VISA International to remedy flaws in their proposed standard for bankcard transactions over the Internet. Such work, up to and including demonstrations of successful attacks, are the accepted method for progress in this field.

Specific Adverse Consequences

If adopted, this ill-conceived amendment would:

- severely impede academic and commercial research aimed at strengthening the security of services offered to citizens and companies;

- make it impossible to hold academic gatherings in Europe discussing these topics, whether of the international scope and prestige of such conferences as EuroCrypt or the Workshops on Fast Software Encryption held at Cambridge University, national gatherings such as those sponsored by Hewlett-Packard at Royal Holloway College London, or purely local gatherings such as the seminar on "Securing the Electronic Transaction" I gave for regional businesses at UWE earlier this week, sponsored by the DTI;

- weaken the fielded security of information systems by allowing sloppy design to go unchallenged by open review, and the spurious reasoning that "no-one will attack this system because to do so would be illegal" — an approach to security which is conspicuously inadequate to prevent other forms of theft!

Inappropriate Legislative Target

As a lawyer yourself, I'm sure you'll appreciate the nonsensical nature of banning an activity which on balance improves our society. What needs to be legislated against — if existing law does not adequately cover it — is the criminal exploitation of security weaknesses in electronic systems. The proposed amendment is analagous to banning motoring on the grounds that some criminals will use cars in committing a crime, or of banning the discussion and testing of photographic techniques since photography can be used to create obscene materials.

UK DTI Not In Favour Of The Amendment

The UK's Department of Trade and Industry is not in favour of this amendment. The senior civil servant responsible for encryption policy, David Hendon, has commented in public to the UK cryptographic community as follows, on 11 March 1998:

> I hesitate to enter this debate, but here goes anyway.
>
> First of all, let me say that the directive that Ross mentions is nothing to do with me and is being handled in another bit of DTI as a copyright protection measure. As the guy in DTI responsible for encryption policy though, I would be just as concerned as Ross if the outcome was as he describes. I haven't looked at the documents yet.
>
> I gather that the state of negotiation of this directive is that it is under-going its first reading in the Council and the European Parliament (EP). Under the Mastricht co-decision procedure, such directives are decided jointly by both institutions, the Council and the Parliament. The co-decision procedure is as arcane a procedure as I ever met in 30 years in the civil service, but the interesting bit for the moment is what happens to EP amendments. Basically, the Council of Ministers - in this case the Internal Market Council (in practice a working group of experts at my level or lower) and the Parliament (a working group of MEPs) separately consider the text as proposed by the European Commission. Normally both the Council working group and the Parliamentary Group propose amendments to the text. Once the Plenary of the Parliament has approved the amendments, the Council and the Commission decide whether to accept them. The Council adopts as a "common position" a text which subsequently goes again to the EP for a second reading. The EP can propose further amendments and it all gets very difficult then if people don't agree what should go into the text.
>
> I will save all that stuff for later. It will certainly be many months

away.

So if you want to kick into touch amendments proposed in a working group of the EP, you need to persuade the MEPs who are in the working group or, even better, the rapporteur for the directive. I don't know who it is at the moment, but I can find out. If the amendments stay in the report of the group, then the next chance is to get them kicked out when the report of the Group is accepted by the superior committee. I don't know for sure which this is, but it is probably what is called EMAC (I think this is economic and monetary affairs committee — they certainly deal with all the telecomms stuff). If the amendments stay in there, then you need to lobby the members of the EP themselves. You need to get academics in other countries lobbying their MEPs as well, because it wouldn't be enough to convince all UK MEPs.

Even if the EP adopt the amendments, it is by no means certain that the Council of Ministers will agree and even if they do the first time round, there is another chance to get the EP to change its position at the second reading. On the face of it, and knowing quite well what other countries' Governments think about encryption, I should have thought the Council of Ministers would never accept these amendments if they really do have the consequences that Ross has outlined because of the implications for European industry in the future.

By the way, the common position in the Council can't be before May and the second reading in the EP therefore won't be until the autumn, so there is quite a bit of time to sort this out. I wouldn't hang about though. It is easier to sort out contentious suggestions as they are made, than months later when they have achieved some sort of status.

Hope this helps.

David Hendon

(The "Ross" to whom David Hendon refers is Ross Anderson, a well-known UK academic cryptographer to whose attention this matter was brought by an unnamed EC official.) Today, 13 March 1998, David Hendon followed up the previous message with the following:

Hi everyone

Further to my posting a couple of days ago, responding to Ross' concerns about possible European Parliament amendments to the draft directive on legal protection of copyright, I have done a bit of digging. It's the Legal

> Affairs Committee of the EP which is considering the amendments and the rapporteur is Giorgios Anastassopoulos. [...]
>
> Anyway, the amendment won't be voted in the Legal Affairs Committee until 14/15 April, so there is a bit of time to lobby MEPs if you want. Having talked to the people concerned here, I gather the DTI won't be supporting that particular EP amendment once it gets to the Council and we don't think the European Commission will either. We have already lobbied the UK members of the EP Committee. Anyone know any Greek companies or academics who could have a word with Mr A?
>
> David Hendon

As you'll see, I'm taking David Hendon's advice and lobbying my MEP!

Action Requested: Please Brief MEP Colleagues As Appropriate

I'd very much appreciate you finding time in your busy schedule to look into the progress of this Directive and its ill-conceived amendment. I am uncertain of the names of the British MEPs who currently serve on the Legal Affairs committee; nor indeed is there any reason that an explanation of the — quite possibly entirely unintended — consequences of this amendment should be restricted to British MEPs. Of the Labour group MEPs, it may be that — based on their committee memberships, stated special interests, and backgrounds — Gordon Adam, Glyn Ford, Mark Hendrick, David Martin, Eryl McNally, Eddy Newman, Christine Oddy, Mel Read, Barry Seal, and Carole Tongue could be interested. (I don't for one moment imagine you'll be able to get round all these people! Moreover, I'm sure you're in a far better position than I to judge their likely level of interest in this issue; nevertheless I hope this initial shortlist might help you identify appropriate colleagues.)

Follow-up Meeting?

In the event that you'd both like and be able to make the time to find out more about this and related information-technology policy issues, I'd be happy to meet either at your Gloucester Road office, or at Hewlett-Packard during the working day. (In closing, I should make it clear that I'm not officially "representing" HP in this matter; however, I do speak with HP's backing in various UK encryption-policy debates together with the director of HPLabs Bristol, Dr John Taylor.)

Thanking you for your attention,

Stefek Zaba