FIPR Response to the Home Office:
"Consultation on the Draft Code of Practice for the Investigation of Protected Electronic Information – Part III of the Regulation of Investigatory Powers Act 2000"

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

Besides our main response to the consultation, which is set out below, FIPR would also like to formally draw the Home Office's attention to the eighth "Scrambling for Safety" public meeting held at University College London on the 14th August 2006.

The meeting was attended by Home Office officials and they will be able to refresh their memory of the talks – and, in particular, read further supplementary material on the human rights aspects of the question of increased sentences for some types of offender – by visiting: **`http://www.fipr.org/sfs/index.html`**.

FIPR does not believe that Part III should be activated at all!

Both decryption powers and access to keys are obsolete. Most encryption products now offer multiple-key disk encryption, a concept pioneered by FIPR Chair Professor Ross Anderson, along with Adi Shamir and Roger Needham in their paper on "The Steganographic File System", which was written in response to early key escrow moves. Such systems let a user create multiple encrypted partitions, without an outsider knowing how many.

A connoisseur of S&M porn might prudently use such a system to encrypt his image collection, with the images under key B and some innocuous private material, such as his tax returns, under key A. If such images are in the future made illegal, as your department proposes, and if his PC then falls into police hands, he can either (if required to decrypt) use password A to show his tax documents, or (if required to surrender a key) give password A to the police. In neither case is the policeman's objective attained. (We note in passing that the political support achieved on decryption powers by talking about child pornography and terrorism will be undermined if your department introduces censorship powers that command much less universal support.)

Thus, regardless of whether you introduce decryption powers only, access to keys, or both, you are unlikely to achieve more than a small and transient increase in your conviction rates, and that only until the criminal community learn how to use the available tools properly. In the meantime, these powers will mostly provide "surrogate offences" whereby criminals can be sent to jail for non-decryption rather

than for possessing unlawful images of child abuse. Surrogate offences are by their nature objectionable; mobsters should go to jail for their real crimes rather than for tax evasion.

If ministers are determined to be seen to be "doing something" by activating Part III, they should still not mandate access to keys. When elected in 1997, Tony Blair promised that there would only be a power to demand decryption; and although the US and the intelligence lobby have worked mightily to shift that stance slightly, we believe that the limitation he introduced into his election platform was wise.

Access to keys will have a thoroughly chilling effect on commerce. This is grudgingly recognised by the special provisions proposed in the Code of Practice for dealing with financial institutions; but, unfortunately, the effects will not be limited to banks, as most businesses of any size do significant business online these days.

The argument is made, in various forms, that in some circumstances the police must demand the key in order to prevent a suspect doing something wicked with his PC when given access to it for the purposes of decryption. The police argument that a pornographer might manage to have one last, longing look at unlawful images as he decrypts them is risible; a better argument might be that encryption systems may be equipped with a duress password that causes the instant deletion of incriminating matter. In our example above, the use of password C might not only decrypt the same material as password A, but also cause everything encrypted under password B to become non-recoverable.

In FIPR's opinion, the best way of dealing with such (largely imaginary) fears is to have, instead of access to keys, a provision whereby the decryption will be performed by the suspect's lawyer. It remains possible that the suspect will deceive his lawyer and cause the lawyer to use a duress key, but if the production of a key is compelled then the suspect can similarly deceive the police into using the duress key, and so nothing is lost by having the decryption performed by a lawyer rather than by a policeman.

The Home Office should also bear in mind that the most successful legislation is technology neutral, as technology moves much faster than law. Access to keys was first mooted (recently) in the USA in 1993, and in the UK by DTI minister Ian Taylor in 1996. It has taken ten years since then to get this far; in the meantime, security vendors have anticipated this legislation and deployed effective ways to avoid it. If what policemen actually need is access to plaintext, then that is the most that the legislator should seek to compel.

FIPR
1st September 2006