Faraday attracts more interest in plans for UK science centres

London. Britain's Labour Party has promised to create a number of 'Faraday Centres' — intended to link the academic and industrial worlds, and named, ironically, after Mrs Margaret Thatcher's favourite scientist, Michael Faraday — if it wins the general election due within the next year.

The party's goal, according to Adam Ingram, the 'shadow' minister for science and technology, is to create "stable institutional structures to facilitate bringing together the various strands of our science base".

But despite a pledge in its manifesto, published two weeks ago, to recognize the importance of science to the economy, the Labour Party has held back from any commitment to increase funding for science — as it has for virtually all other areas of public spending.

The idea of creating Faraday Centres was first proposed by the Conservatives just before the last general election in 1992, based on a suggestion by a working party set up by Prince Charles that Britain should develop institutions similar in function to Germany's Fraunhofer Institutes.

Soon after, the Labour Party came up with its rival project for so-called 'Newton Centres'. But after the Conservatives won the election, the Faraday concept was dropped by the then president of the Board of Trade, Michael Heseltine.

In recent months, the Conservative government has again been promising to set up a small number of centres, aimed at providing focal points for interaction between the private sector and the publicly-funded research community.

Labour now seems keen on a similar idea. It has dropped its earlier insistence that these be new, free-standing institutions, and accepted that they should be based on existing research centres. Ingram says that Labour is keen to use public sector research establishments as a nucleus.

He also says that he has found a high level of enthusiasm in private industry, spurred in particular by the government's Technology Foresight exercise. "There seems to be plenty of interest from the private sector in fields such as aeronautics, space and marine research, materials, the chemical industry and pharmaceutical research," he says.

David Dickson

Faraday: name used by political rivals.

Network crime prompts UK moves on access to data

London. The British government is planning to give itself powers to access encrypted information stored on — or passing through — computer networks, according to proposals set out last month by the Department of Trade and Industry (DTI).

The move follows concern among Britain's intelligence agencies over a perceived increased use by criminals of sophisticated encryption software to conceal information used in unlawful activities such as computer pornography and fraud.

It also coincides with a renewed attempt by the United States government to introduce the so-called 'key escrow' system, after earlier moves in this direction had been dropped. A cabinet-level committee is to propose new encryption recommendations to President Bill Clinton by early September.

But the UK proposals are being viewed with concern by professional bodies such as the British Medical Association (BMA), which highlights the potential loss of privacy for lawful users of encrypted public networks, such as the National Health Service.

If the proposals become law, any individual or organization intending to send or store encrypted information on a network linked to an external telephone line will be required to provide copies of the decryption passwords — known as keys — to licensed independent organizations, known as 'trusted third parties'.

Government departments and intelligence agencies will — on production of a court order to the appropriate third party — be allowed access to these keys if they need to monitor encrypted information. This system is referred to as 'key escrow'.

The scheme is in line with identical proposals put forward by the European Commission (EC) last August (see *Nature* 377, 275; 1995). Parts of it are also similar to key escrow proposals put forward in the United States by the Clinton administration in 1993, but strongly opposed by civil liberties organizations and business groups.

Although civil liberties groups in the United Kingdom are similarly opposed to the British proposals, the government has been careful not to irritate the business community. The DTI scheme, for example, will not permit access to encrypted information on private-company mailing lists or in closed computer networks such as those between banks and their customers. "It is not the intention of the government to stifle competitiveness," says a DTI spokesman.

But not all potential critics have been satisfied. The BMA is deeply opposed to the idea of government access to encrypted data. The proposals have fuelled a dispute between the BMA and the Department of

Health about the security of a planned computer network for the health service which will allow networked storage and retrieval of patient records.

Criticism has also focused on suggestions that the General Medical Council (GMC), the doctors' regulatory body, could act as the third party to release decryption keys.

Ross Anderson, a lecturer at the University of Cambridge Computer Laboratory and an adviser to the BMA on information security, says the proposal to ask the GMC to hold decryption keys would transform it from a body charged with upholding professional standards into one responsible for disclosing personal health information to the security services. "I cannot imagine a proposal more likely to destroy the high level of trust that the [council] currently enjoys from both professionals and patients," he says.

Gunnar Klein, who chairs an EC working party drawing up a common standard for European health-care information networks, says he does not see how government access to confidential patient records will help to prevent the passage of information used in illegal activities.

Klein finds the UK government's regulatory approach inconsistent. The proposals, he says, do not give the government the right to intercept illegal information on large, country-wide private computer networks, "such as those set up by terrorist groups like the IRA [Irish Republican Army]". But, he says, "they allow the intelligence agencies access to confidential medical records that have no relevance to crime".

Under the new US proposals, the government has agreed to temporarily lift the ban on the export of stronger — but non-escrowed — encryption products that use a key length of 40 bits. (The strength of a product is measured by the length of its key.) But in return, software manufacturers will be asked to drop their opposition to key escrow and incorporate it into future encryption products.

Software companies have been concerned that the government's key escrow proposals would jeopardize their US\$600 million revenue from exports of encryption software. Manufacturers pointed out at the time that international customers were unlikely to buy products that would entitle the US government to eavesdrop on them.

Vice President Al Gore said the administration will not be supporting a Republican bill that calls for the lifting of export controls on all encryption software. "We do not want to do anything that would damage our own national security or public safety by spreading unbreakable encryption."

Ehsan Masood