You've got mail! (and so have weeeee...!)

After rejecting intelligence agency plans to require computer users to "escrow" their secret keys to provide police access, the Prime Minister has given civil servants and computer experts until April 1 to suggest alternative ways for police and security agencies to monitor the Net. Could the new solutions be worse than the old, asks Duncan Campbell. And are they already in use?

By Duncan Campbell

***Guardian*, Thursday March 18, 1999**

In the Australian report, Walsh even considers whether the government should create a second intelligence agency to monitor communications. But he rejects the proposal, likely to cost A250 million, as too expensive to justify.

In the US, senators last year proposed turning NSA inwards by linking it to the proposed new NET Center. Their bill proposed that the new centre would work with NSA to 'conduct research to develop efficient methods of accessing plain text of communications and electronic information', and to 'investigate and research new and emerging techniques and technologies to facilitate access to communications and electronic information'.

Britain's surveillance centre, GCHQ, has already been given powers to do everything that Walsh proposes. The 1994 Intelligence Services Act sets out GCHQ's prime function as being 'to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions in support of the prevention or detection of serious crime'. Interference requires a warrant from a Secretary of State.

Unlike Walsh in Australia, however, the British act does not consider the legal position of someone whose computer systems, information or business activities might be damaged or destroyed by a government information warfare attack. Walsh

implies that the government ought to regard itself as liable for the consequences of an electronic attack on a surveillance target. American opponents of the NET Center say the proposal, if approved, 'would constitute a fundamental re-definition of the relationship between intelligence agencies and domestic law enforcement'. The Electronic Privacy Information Center, a lobby group based in Washington, says 'such an approach would ignore 50 years of experience and would pose a serious threat to privacy and constitutional rights.' Diffie adds: 'Signals intelligence has risen steadily in importance throughout this century. It's a robust phenomenon. The driving force is how much people communicate. This could evolve to circumstances where a machine analyses [everything found on computer disks] - then you would have mechanised mass surveillance.' 'Such things are possible,' he warns. 'None of the security mechanisms on current computers are good enough to withstand the best attackers.'