

FOUNDATION FOR INFORMATION POLICY RESEARCH

www.fipr.org

9 Stavordale Road
London N5 1NE
Tel: 0171 354 2333
Fax: 0171 827 6534
E-mail: cb@fipr.org

The Foundation for Information Policy Research is an independent non-profit organisation that studies the interaction between information technology and society, with special reference to the Internet, from a broad public policy perspective; we do not represent the interests of any trade-group. Our goal is to identify technical developments with significant social impact, commission research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers.

“UNPRECEDENTED SAFEGUARDS FOR UNPRECEDENTED CAPABILITIES”

Presented at the Hoover Institution at Stanford University, National Security Forum Conference, “International Cooperation to Combat Cyber Attacks”. 7th December 1999

ABSTRACT

We recapitulate UK policy history on interception and cryptography, including consultations on key escrow and proposed extension of interception powers to cover the Internet. We then discuss how the systematic capability for Internet surveillance envisaged raises not only technical and cost issues, but strains current frameworks for authorisation, oversight, and accountability.

The Foundation for Information Policy Research is registered in England and Wales as a private company limited by guarantee (No.3574631). Application for charitable status is in progress.

Members of the Board of Trustees - Chair: Dr. Ross Anderson (Cambridge Computer Laboratory), Andrew Graham (Acting Master, Balliol College Oxford), Dr. Fleur Fisher (formerly BMA), John Wadham (Liberty), Prof. Roger Needham (Microsoft Research UK), Tim Jones (NatWest), Prof. Peter Landrock (Cryptomathic)

Form SF298 Citation Data

Report Date <i>("DD MON YYYY")</i> 07121999	Report Type N/A	Dates Covered (from... to) <i>("DD MON YYYY")</i>
Title and Subtitle Unprecedented Safeguards For Unprecedented Capabilities		Contract or Grant Number
		Program Element Number
Authors		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042		Performing Organization Number(s)
Sponsoring/Monitoring Agency Name(s) and Address(es)		Monitoring Agency Acronym
		Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Document Classification unclassified	Classification of SF298 unclassified	
Classification of Abstract unclassified	Limitation of Abstract unlimited	
Number of Pages 8		

REPORT DOCUMENTATION PAGEForm Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 12/7/99	3. REPORT TYPE AND DATES COVERED White Paper	
4. TITLE AND SUBTITLE Unprecedented Safeguards For Unprecedented Capabilities			5. FUNDING NUMBERS	
6. AUTHOR(S) Not provided				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church, VA 22042			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Technical Information Center DTIC-AI 8725 John J. Kingman Road, Suite 944			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) We recapitulate UK policy history on interception and cryptography, including consultations on key escrow and proposed extension of interception powers to cover the Internet. We then discuss how the systematic capability for Internet surveillance envisaged raises not only technical and cost issues, but strains current frameworks for authorization, oversight, and accountability.				
14. SUBJECT TERMS Cyber, interception, cryptography, key escrow			15. NUMBER OF PAGES	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified		20. LIMITATION OF ABSTRACT Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

UK POLICY HISTORY

The UK government last month published its long awaited Electronic Communications Bill, which emerged from a three-year struggle over the control of encryption, largely shorn of its most controversial clauses.

In 1996 the previous administration proposed a system of mandatory "key escrow" - the surrender to a third-party organisation of spare keys to unlock data, in case required by the police. Responses from industry and the Internet community to a consultation in 1997 were vitriolic, for both technical and commercial reasons. After the May 97 election, although key-escrow had been rejected by the Labour party in opposition, after a year's delay they offered coercive inducements for "voluntary" escrow. Another year passed before key-escrow was excised from a second public consultation, after intervention from the Prime Minister.

A Draft Bill published in June contained draconian new law-enforcement powers to demand decryption keys from anybody by serving a written "notice" (rather than a warrant). Prosecution for withholding a key would have a presumption of guilt, unless the defence could somehow prove non-possession. The Home Office argued that being asked to provide a decryption key was just like requiring a DNA sample - but even a person not suspected of any crime who had lost or forgotten their key would have had to convince the court or go to jail for two years.

Decryption notices could be served on associates, legitimate third-parties, and legal advisers, with an obligation not to change keys if this would "tip-off" the suspect. The most chilling provision was that notices could contain a total obligation of secrecy - preventing anyone from complaining publicly (for example to the newspapers), with a penalty of five years imprisonment.

Ingeniously crafted for minimal compliance with a 1984 Commission on Human Rights ruling, the 1985 Interception of Communications Act (IOCA) created a Tribunal that cannot even investigate illegal (unwarranted) tapping, and can only uphold a complaint if it was "manifestly unreasonable" to issue a warrant. Otherwise the Tribunal doesn't tell complainants whether or not they were intercepted, on the grounds that interception is most effective when shrouded in secrecy. For the same reason, intercepts are not admissible as evidence in court (but many senior police officers now want to be able to use wiretaps in evidence, as in the United States).

In the Draft Bill, a complainant's only recourse was to a Decryption Tribunal, which could hold proceedings in their absence, and even flagrant breaches of a code of practice by authorities with access to keys, would not have been a criminal offence. These issues were being dealt with in an e-commerce bill, because the government wished to bolt on decryption powers to the existing interception and seizure laws. The Home Office feared that if the current Catch-22 framework of authorisation unravelled, they faced a policy meltdown.

The analogy was frequently used that there is no difference in principle between an encrypted document and a locked safe.¹ However, aside from the obvious difference that a physical safe can usually be forced open, if an encrypted message is camouflaged using the techniques of steganography, the analogy with existing search and seizure law breaks down completely. In this situation, no-one knows whether there is a safe, let alone whether there is a key.

Human Rights

FIPR believed that the effective reversal of the presumption-of-innocence would be likely to contravene the European Convention on Human Rights. This conclusion was substantiated when FIPR and the legal-rights organisation JUSTICE commissioned a legal Opinion from a leading human rights lawyer (QC and Cambridge professor of law and former law commissioner) to assess whether the Bill was 'human rights compliant'.

Their advice was that it was not: the UK government had wrongly opted for the widest police powers. According to the Opinion, this "will have the inevitable consequence of compromising the affected individual's whole security and privacy apparatus" and likely contravene Article 8 of the European Convention, on respect for private life. The Opinion confirmed that the reverse-burden-of-proof was likely to violate Article 6, on the right to a fair trial. Moreover, the provisions in the Bill requiring a suspect to turn over an encryption key violate the right not to incriminate oneself, also protected under Article 6.

Decryption Powers: R.I.P ?

The powers to issue decryption notices and the obligation-of-secrecy ("tipping-off") offence have disappeared from the final E-Comms Bill. However the government has not (so far) acknowledged any human-rights contravention, and these provisions may re-appear in a new 'Regulation of Investigatory Powers Bill' from the Home Office, which will regulate all covert police methods from the use of informers to Internet surveillance.

It is natural to ask, if previously proposed decryption powers were unsatisfactory in an e-commerce bill, why should anyone think they are acceptable in a law-enforcement bill? Although industry understands that encryption is a routine and necessary tool for e-commerce, there may be a calculation that industry objections may be attenuated if portrayed as being soft on crime. The press release accompanying the launch of the new Bill referred to "paedophiles, drug-traffickers and terrorists" using the "deadly weapon" of encryption².

Interception, Decryption and Intrusive Surveillance

The inter-relationship of interception, decryption and surveillance (video/microphone/computer-virus) is extremely complex. A decryption warrant served on a suspect precludes covert

¹ 'Communicating Britain's Future', (The Labour Party 1995) available at <http://www.liberty.org.uk/cacib/legal/crypto/labour2.html>.

² Joint DTI/Home Office Press Statement on publication of E-Comms Bill (19/12/99)

FOUNDATION FOR INFORMATION POLICY RESEARCH

investigation, but covert access to keys may in certain situations be provided by intrusive surveillance. The interaction was excluded from the scope of separate UK public consultations on Internet interception and decryption powers earlier this year.

At present the authorisation, oversight and accountability of various forms of search and surveillance differ drastically. For interception, an eminent judge (the “Commissioner”) makes spot-checks and has never reported serious abuse, but has no technical staff and depends on the law enforcement agencies he is overseeing to tell him what is happening. Search warrants may be issued by magistrates or the police depending on circumstances, and intrusive surveillance is self-authorised by senior police officers.

FIPR believes that to oversee interception in the Internet age, the Commissioner's office needs an independent investigatory capability with technical staff, and the mandate to pro-actively deal with unwarranted tapping. There is now also the best opportunity in a generation to reform the existing patchwork of laws to establish a consistent system of surveillance authorisation with effective technical and legal safeguards.

In 1998 the Home Secretary issued more than two thousand interception warrants (an average of seven every business day). Normal statistical fluctuations would suggest that on many busy days at least double this number must be authorised. The constitutional position is that “each warrant is personally authorised by the relevant Secretary of State...and only when he or she is satisfied that it is strictly necessary”³, which must include inquiries as to whether the information could not reasonably be obtained by other means. The Home Secretary has declined to say how much time a typical authorisation occupies, reasonable assumptions about necessary diligence suggest a daily regimen of at least 30 to 120 minutes of warrantry formalities: an heroic daily burden.

A Tribunal of appointed senior lawyers deals with complaints about interception. Since 1986, it has considered 568 complaints. However in only 8 of these cases was a warrant in force, and the Tribunal thus empowered to conduct an investigation. Although in none of these cases was a contravention of the Act found, since the total number of warrants issued since 1986 perhaps numbers 20,000, there is no statistical basis for reassurance.

A leading academic commentator has described the current Act as “an insult, and a cynical insult.... it must be remembered that the ‘criminals’ may well be an elite group within the police or the security service - detection is likely to be an impossibility. The Act secures that there is no likelihood apart from the tribunal, of civil redress against a secretary of state who is in breach of the authorisation provision or against an official who has conducted an unauthorised interception.”⁴

³ “INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM” - Home Office consultation paper (CM 4368 JUNE 1999)

⁴ p.43 *Freedom of Information: The Law, the Practice and the Ideal* (2nd ed), Patrick Birkinshaw, Butterworths 1996

PROVISION OF “REASONABLE” INTERCEPT CAPABILITY

The 1999 consultation on extending interception powers proposed that all “Communication Service Providers” (CSPs – which include ISPs and licensed telcos) must provide a “reasonable interception capability” – which was not further defined.

There are two technical extremes within which any intercept capability must be defined. Only “application layer” data (e.g. e-mail, Web pages, chat) is readily intelligible, and is decomposed and re-assembled through many logical layers of software which implement the various communication “protocols” and interpret data formats. At the other extreme, Internet data is ultimately transmitted as a stream of small packets called *datagrams* through the switching equipment of the Internet Service Provider. Each datagram contains an address field to route the packet to its destination. Intermediate level protocols deal with lost packets, and network control information.

A computer which connects to the Internet through a dial-up service may register its caller-ID information in a log file, together with an “IP” address (fixed or varying) allocated for that session. The Internet Service Provider may be able (with difficulty) to deliver a copy of the packet stream for a given user’s online session, although this may require special handling depending on network size and configuration. It will generally be impossible for the ISP to reconstruct application layer data, unless the ISP’s own computers are running the corresponding service (e.g. e-mail); even so, special configuration or custom programming may be required, and it may be infeasible to thwart all active strategies for detecting interception.

For small and medium-size ISPs, even delivery of a filtered target packet stream may prove extremely disruptive and onerous. As the Internet interception debate evolves, we foresee a temptation for government to offer “black-box” solutions for attachment to provider’s networks, which would undertake data collection under remote control. The Russian security service (FSB) has reportedly already imposed such requirements⁵. FIPR believes that to maintain public confidence, the selection, acquisition and filtering of targeted traffic must always remain under ISP control, and they should always be in a position to verify that data abstracted strictly complies with the presented warrant. interception. However for small ISPs, even providing the most basic e-mail and filtered sniffing capability will prove skilled-labour intensive and one of the largest UK ISP’s has estimated that compliance could increase their costs by 10%.

The United States has recently proposed a system for comprehensive domestic Internet monitoring, modelled on military lines, through creating network access points throughout the *private sector* infrastructure, for purposes of critical national infrastructure protection⁶. This has immediately given

⁵ <http://www.jya.com/sorm-en.htm>

⁶ <http://www.cdt.org/policy/terrorism/fidnet/>

rise to fears that it may be used for untrammelled surveillance, and appropriations for the program have reportedly been suspended.⁷

Recently the IETF has been discussing whether it should formally take on the role of designing law-enforcement access into new Internet protocols. The debate is at an early stage, but an important question that must be considered is who will hold the keys to any such back-doors? Similar multilateral discussions a few years ago could not reach agreement on jurisdiction and procedures to “extradite” a key held in escrow by another state. National security interests are unlikely to be comfortable with the idea that back-door keys to access the infrastructure could be released to foreign law-enforcement agencies.

WARRANTY PROCEDURES

The argument offered in support of continuance of Secretary of State authorisation is that Executive approval is needed for national security cases. The Royal Commission on Criminal Procedure⁸ recommended a uniform system of judicial warrants (and subject notification) for all forms of surveillance even before the Malone 1984 ECHR case necessitated legislation. JUSTICE⁹, Liberty (formerly NCCL), and most recently the Data Protection Registrar have all advocated similar reforms:

“...the Registrar is unhappy with the current situation because IoCA warrants are not subject to judicial scrutiny either at the point of issue or, because the information obtained is not admissible as evidence, by a court at a later date, and she believes that it is now time to amend IoCA so that an application for a warrant to obtain this type of information is subject to judicial consideration.”¹⁰

FIPR’s position is that uniform judicial authorisation, although it may require some re-organisation and extra training within the judiciary, presents no special difficulties.

The 1999 IOCA consultation also proposed allowing subsequent addition of extra ad-hoc “addresses” to a warrant by officials. The appending of unidentified Internet accounts, or sub-netted/translated/spoofed IP-addresses of uncertain provenance, to warrants of extended duration, by civil servants inured to a daily diet of communications villainy, could be the last straw which breaks the constitutional convention of direct ministerial accountability to Parliament. Application to obtain or modify a judicial warrant should instead present reasonable evidence that the targeted account relates to the investigation in the way claimed – typically this may involve analysis of traffic (communications) data.

⁷ House majority leader, Rep. Dick Arney said FIDNET raised “the Orwellian possibility that unscrupulous government bureaucrats could one day use such a system to read our personal e-mail.” *New York Times*, 28th July 1999

⁸ *CM 8092*, Jan 1981, chaired by Sir Cyril Phillips

⁹ *Under Surveillance: Covert Policing and Human Rights Standards*, JUSTICE 1998

¹⁰ *the fifteenth annual report* Data Protection Registrar, , June 1999, para.19

TRAFFIC DATA

The consultation proposed putting access to traffic data on a statutory basis (presently the police make informal requests), but appeared to recommend the abolition of Data Protection Act safeguards requiring law-enforcement to demonstrate fulfilment of criteria such as necessity for an investigation.

There are now traffic-analysis tools commercially available to law enforcement which can take telephone number logs in machine-readable form and draw "friendship trees" which show the grouping and relationships between parties calling each other in time, and can match patterns of association automatically using sophisticated artificial intelligence programming.

There is enormous potential for law enforcement in increased use of traffic analysis, but there are a number of fundamental distinctions between traffic analysis of telephony, and Internet traffic – especially in a fully wired Information Society. The Internet Protocol ("IP") abolishes any meaningful distinction between domestic and foreign communications intelligence. A well-funded national communications intelligence agency which already captures large quantities of both traffic and content data, and has the organisation to process it and integrate it effectively with other forms of intelligence gathering, presents an enormous temptation to government simply to leverage that capability for wider domestic coverage.

Intelligence-integrated traffic-analysis is phenomenally corrosive of civil liberties. If government was in a position to know which websites you visit, what you buy online, the e-mail addresses of those who e-mail you and those you have e-mailed, and analyse and archive that information without hindrance, there is potential for an unprecedentedly serious abuse of power.

“Trawling warrants” for foreign communications intelligence specify a logical circuit or domain of capture, rather than topic or person. The idea is that signals are vacuumed up, untouched by human hands, and then automatically selected by computer against a “certificate” issued by the Secretary of State that actually contains the description of the target subject matter (suitable for machine searching). The Secretary of State must guarantee that “intercepted material [which] is not certified . . . is not read, looked at or listened to by any person”. Appeals to a Data Protection Tribunal against the issuing of a certificate are possible, however the Data Protection Registrar has persistently criticised national security exemptions:

“...As far as we have been concerned, under the 1984 Act exemptions from the law are only on a case-by-case basis, although the exemptions for national security are broader. I have had some concerns about the definition of national security for data protection purposes and whether perhaps too broad an exemption has been claimed. It is something I wrote to the Secretary of State about, both under the previous Government and under the present Government. Indeed, we are hoping that some review of that boundary will be undertaken before the 1998 Act comes into force.”¹¹

¹¹ Mrs. Elizabeth France, Data Protection Registrar, Minutes of Evidence taken before the Trade and Industry Committee, 9th March 1999, para.480