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

16th August 1999

To: ioca@homeoffice.gsi.gov.uk

The Interception Legislation Team
Organised and International Crime Directorate
Room 735
Home Office
50, Queen Anne's Gate
LONDON SW1H 9AT

INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM

A response to the Home Office consultation paper (CM 4368 JUNE 1999)

BY THE

FOUNDATION FOR INFORMATION POLICY RESEARCH

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 in the UK and Europe.

FIPR has been influential in raising public awareness of technical matters prerequisite to an appreciation of difficult policy choices, through public meetings and briefings with journalists, MPs, officials, and industry groups.
(Late submission on 16/8/99 agreed on 13/8/99 by telephone with Nicola Carnie, OICD Home Office)

Permission is granted for publication of this response.

EXECUTIVE SUMMARY

Those who question the arrangements for oversight of interception are often supposed to be critical of the rights of the state to conduct secret surveillance. FIPR supports carefully targeted government surveillance of telecommunications in the fight against serious crime and for the collection of foreign intelligence.

However public support for these activities has been very seriously eroded by the poor management of previous governments - not just by the wiretapping of organisations such as the NCCL and Amnesty, but also by enacting surveillance legislation with meagre safeguards providing token redress, and consistently doing so only when obliged by adverse human-rights judgements, to a minimum standard of compliance[1].

This submission will primarily deal with issues arising from the proposed extension of IOCA 1985 powers to cover interception of the Internet. The systematic capability for Internet surveillance envisaged by the Home Office raises important technical and cost issues for the industry, which directly relate to the adequacy of arrangements for oversight, accountability, and data protection.

The proposals lack detail, and show no technical appreciation of fundamental distinctions which differentiate the structure and protocols of the Internet from point-to-point telecommunications networks designed for voice traffic. To achieve a workable consensus, we believe that it will be necessary for the government to consult further when they are in a position to define what constitutes a "reasonable" intercept capability in typical cases, and to publish a draft of the Code of Practice.

Since the Government's intention was to introduce the Electronic Communications Bill in the previous session of parliament, we are disappointed that there is no discussion of cryptography in this consultation, and the intricate interactions with interception policy.

Now that the Electronic Communications Bill is open for further consultation, we will defer a detailed discussion of the connections between cryptography and interception until our response in October. However we believe it is desirable to promote an early recognition by Government that the combination of powerful economic forces and new cryptographic techniques are likely to place current frameworks for authorisation, oversight, and accountability under immense strain, and raise unprecedented civil liberties issues for domestic interception policy.

[1] "…one of this Government's 'dumb insolence' measures . . . in which the minimum action possible is grudgingly taken to comply with the letter of rulings under international agreements." *The Times*, 6 March 1985

The causes may be external and technical, but the real challenges are institutional:

- the Data Protection Registrar has now unambiguously adopted the position that Secretary of State warrantry should be replaced with judicial authorisation in all cases.[2]

- asymmetric cryptography over the Internet nullifies the possibility of covert interception and decryption without severely compromising the human rights of innocent associates (second parties) or the trusted role of intermediaries (third-parties), in ways which are **not** analogous to telephone interception.[3]

- oppressive proposals for decryption notices could actually accelerate the deterioration of law-enforcement capabilities for interception and seizure of evidence, by encouraging deployment of anonymity and steganography tools with plausible deniability. Effective reversal of the presumption of innocence, and imposed obligations of secrecy are an affront to the technically literate community whose co-operation is required to police the Internet by consent.[4]

- although the IOCA consultation paper discusses traditional arguments for and against repeal of Section.9, it appears little account has been taken of the rapid migration of voice telephony towards IP ("Internet Protocol"), the near prospect of UMTS devices which would support tunnelling and anonymity, and the consequent likely need for corroborative traffic and content evidence admissibility to secure safe convictions under existing and envisaged legislation.

- the Government believes that these issues are tractable within the current framework. Their view of policy development has repeatedly proven mistaken (it appears because of a wholly inadequate technical grounding) over the past three years.

[2] "…[in] circumstances in which it is open to law enforcement agencies to look at encrypted messages… I would like those to be closely controlled and I would like us to be looking to judicial warrant…" *Data Protection Registrar, Minutes of Evidence taken before the Trade and Industry Committee, 9th March 1999, para.482*

[3] "it may be they would have justification for intercepting without the knowledge of the person sending the message; and in those cases I would be very concerned about the possible compromising of the key; and I would like us to consider whether in fact that is ever necessary, or whether the warrant could be applied where appropriate to the trusted third party and the information provided to the law enforcement agencies in plain text." *ibid*. –[the DPR did not take a definitive position when a key is not held by a TTP.]

INTRODUCTION

We note that that more than two thousand interception warrants were issued in 1998, which equates to an average of seven every business day. Normal statistical fluctuations would suggest therefore that on many busy days at least double this number must be authorised. The consultation document is introduced with the Home Secretary's written assurance 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", which must include inquiries as to whether the information could not reasonably be obtained by other means. When asked at the launch Press Conference how much of his time a typical authorisation consumed, the Home Secretary modestly declined to answer, and instead stressed the oversight role of the Commissioner. Assuming that necessary diligence would require personal scrutiny of each application for between five and fifteen minutes, a daily regimen of at least 30 to 120 minutes of warrantry formalities is an heroic burden which should not escape commendation.

The Tribunal is kept less busy. The 1997 report of the Commissioner states that that since it was established in 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. Although the Commissioner is known to operate random spot-checks, there is no information on their rigour relative to Tribunal investigations, or whether they provide a sufficient sample for statistical confidence.

We welcome the Home Secretary's acknowledgement that "disproportionate, or unfettered, use of interception can have consequences for the rights of individuals", but note that current safeguards do not permit the Tribunal to uphold a complaint if use of interception was in fact disproportionate in an individual's case – it may only consider whether on the facts presented at the time it was reasonable to grant a warrant.

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."[5]

In fact, the IOCA 1985 bill was debated in a febrile atmosphere created by the revelations of ex-MI5 officer Cathy Massiter, who revealed on Channel 4 television[6] that during the mid-1970s, the National Council for Civil Liberties and a number of other campaigning groups were targeted as 'subversive' organisations and placed under surveillance. The Home Secretary asked

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

[6] *MI5's Offcial Secrets*, 20/20 Vision, Channel 4, 8 March 1985

Lord Bridge (the "Judicial Monitor" for interception) to investigate under "ludicrously inappropriate terms of reference"[7], leading a former Home Secretary to write to 'The Times':

> "A judge of status and quality ought not, in my view, to have agreed to conduct such an enquiry within the limitations of time and scope imposed by the Prime Minister. He has made himself appear a poodle of the executive."[8]

PROVISION OF "REASONABLE" INTERCEPT CAPABILITY

From the point of view of the Internet community, the central difficulty in responding to the consultation paper is that the concept of Internet interception is not defined. It is only proposed that "reasonable" steps are taken by CSPs, to be determined in the first instance by OFTEL, and ultimately the Secretary of State.

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.

As far as we are aware OFTEL has no experience, technical or commercial, of ISP operations, systems or networks. We would prefer to see the establishment of a new Advisory Committee, composed of representatives not only from service providers, but also the user and technical communities, with OFTEL as one participant. Internet technical standards evolve with extreme rapidity through open peer review. Unless the government is content to receive a simple packet-stream which it is prepared to reconstruct into application data without assistance, attempting to exclude any group of stakeholders would be counter-productive.

---

[7] *Stranger On The Line: The Secret History of Phone Tapping*, Patrick Fitzgerald and Mark Leopold, The Bodley Head 1987, p.151

[8] Rt. Hon Roy Jenkins MP, letter to *The Times*, 12 March 1985

An issue which particularly concerns us is that 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 requirements[9]. We believe 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. We recommend that government examines the possibility of serving warrants at different positions in the dendritic backbone: it should be possible in many circumstances to obtain local CLI/IP-assignment data from the dial-up ISP, but take the packets from upstream routers where backbone providers would be better able to service interception requests. However this strategy would require satisfactory procedures to ensure that the IP-address requested upstream corresponded to the target subscriber's account.

We note that 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 protection[10]. This has immediately given rise to fears that it may be used for untrammelled surveillance, and appropriations for the program have reportedly been suspended.[11]

The proposal that ISPs should bear the set-up costs for interception facilities is astonishing. We cannot tell if this is simply a disingenuous negotiating gambit, or based on a fundamental ignorance of the technical differences between PTOs and ISPs. Under the most benign construction we feel obliged to point out that under the CALEA[12] legislation, the US Government allocated a sum of $500m to subsidise the transition to digital telephony interception. For Internet interception, particularly for small ISPs, even providing the most basic e-mail and filtered sniffing capability will prove skilled-labour intensive and proportionately far more costly.

INTERNATIONAL DEVELOPMENTS

We have come across reports of negotiations under MLA to provide international "emergency" warrants designed to compel national ISPs to initiate logging or tracing of target data passing through their systems, for retrospective collection when duly processed authorisation is obtained. This is not explicitly referred to in the paper, and clarification would be welcome.

---

[9] http://www.jya.com/sorm-en.htm
[10] http://www.cdt.org/policy/terrorism/fidnet/
[11] House majority leader, Rep. Dick Armey 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
[12] http://www.cdt.org/digi_tele/cryptovscalea.html

In the two draft MLA Convention cases referred to in 6.2, it is not clear why the "double-lock" safeguards should only apply in the second case. This may refer to technical features of satellite telephony, but clarification would be useful.

Regarding the ENFOPOL proposals, we would also appreciate confirmation of the assertion by Luigi A. Florio, in the Opinion for the Committee on Civil Liberties and Internal Affairs, that "this proposal was originally put forward by the UK"[13]. There is an apparent inconsistency with the statement made by the Home Office Minister in the Explanatory Notes (to ENFOPOL 98 Rev 2) that "the Government sees little need for the draft resolution at the present time"[14]

WARRANTRY PROCEDURES

The sole argument offered in support of continuance of Secretary of State authorisation is that Executive approval is needed for national security and economic well-being cases. This side-steps the satisfactory "parallel" arrangements that exist for judicial PACE warrants. (In any case there does not appear to be any insurmountable constitutional difficulty in judges making decisions on national security or foreign intelligence gathering).

The Royal Commission on Criminal Procedure[15] recommended a uniform system of judicial warrants (and subject notification) for all forms of surveillance even before the Malone 1984 ECHR case necessitated legislation. JUSTICE[16], 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."[17]

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 proposals to allow multiple "addresses" on each warrant and subsequent ad-hoc modification may result in some temporary easing of the embarrassing pressure on Executive authorisation, but the total number of warrants has inexorably (and exponentially) increased since WWII. It underlines the spread of interception since Birkett, who recommended that each warrant be confined to a single person and single address or telephone number.

---

[13] http://www.fipr.org/polarch/euintercept.html
[14] See also *THE GOVERNMENT'S RESPONSE TO THE TRADE AND INDUSTRY COMMITTEE'S REPORT*, para.42
[15] *CM 8092*, Jan 1981, chaired by Sir Cyril Phillips
[16] *Under Surveillance: Covert Policing and Human Rights Standards*, JUSTICE 1998
[17] *the fifteenth annual report* Data Protection Registrar, , June 1999, para.19

The appending of obscurely named Internet accounts (fgyutr12@33zap.net), 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, is a recipe for rapid loss of ministerial accountability. Under present arrangements for oversight with a "judicial review" test, it would be likely prove oppressive and undemocratic.

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.

ADMISSIBILITY OF INTERCEPTS AS EVIDENCE [CHAPTER 8]

> "wiretaps can be extremely valuable as they capture the subjects' own words, which generally holds up much better in court than information acquired from informants, for example, who are often criminals themselves and extremely unreliable"[18]

To date, no satisfactory arrangements have been found. Nevertheless, the Government continues to work on the question, and would welcome the views of others. The Government welcomes suggestions for a regime which would enable intercept material to be used in evidence and to make appropriate disclosures to the defence, bearing in mind the effects upon sensitive information, resources and the efficient operation of the criminal justice system.

The "take" from voice-intercepts is likely to remain substantial for some time to come, irrespective of both landline and mobile telco industry trends towards IP-backbones, because mobile devices will probably remain accessible to interception at their relay stations, as will link-encrypted digital landline traffic.

The outlook for Internet traffic is less clear; much depends on international factors, and business and consumer sentiment. However, it does seem likely that increasingly simplified strong encryption systems will continue to proliferate, and may increasingly be adopted for messaging, and some voice communications (with the arrival of xDSL and UMTS). The Australian Walsh report suggest that Agencies are making preparations to tackle encryption at the endpoints, which will prove much more costly and potentially hazardous to operational security.

On balance it seems clear that admitting evidence from digital intercepts may well be of valuable assistance to law enforcement. If evidence is admitted, it is right and necessary that it should be fully disclosed to the defence under "equality of arms" principles, and its forensic weight assessed. Moreover, many other jurisdictions have operated with full admissibility for many years with no noticeable or qualitative difference to the overall law-enforcement picture.

The counter-argument, that regular use of intercept evidence would educate criminals to take effective counter-measures needs to be unpacked. Some categories of criminal, using some communications systems, may indeed change their behaviour, but presumably lessons will also

[18] *Hiding Crimes in Cyberspace*, Dorothy E. Denning and William E. Baugh, Jr., to appear in Information, Communication and Society, Vol. 2, No 3, Autumn 1999

be learned by the authorities about how the trade-offs change with evolving technologies and counter-counter-measures. Unless law-enforcement takes the plunge, and begins to develop techniques for forensic acquisition and competent presentation of intercept evidence, it will be left hopelessly far behind.

Understanding of asymmetric encryption and related technologies for anonymity and steganography could play an increasingly important role in the investigation of some serious crime. In many cases, the only way to establish a strong case will be to present a hybrid pattern of both communications (traffic) and (possibly encrypted) content data, which will require great care and skill.

OVERSIGHT AND REDRESS [CHAPTER 9]

The Government invites comments on the oversight and redress mechanisms described above and suggestions for how their operation might be improved, bearing in mind the effects upon sensitive information and techniques.

> "Serious thought does need to be given to the following points: do complaints procedures in the UK legislation need strengthening; should oversight be allowed of operational activities; should there be publication at 10-year-intervals of details of the major activities of the services? These would include interception warrants, numbers of complaints referred to the tribunal, numbers of positive vetting referrals handled, an account of the services' opinion on threats and priorities in the relevant period; a case history relevant to the services' work from each branch; and a statement from each director etc relating to any significant changes to practice." [19]

John McWiliam MP, a former post-office engineer had earlier raised a more cynical consideration:

> "If the Tribunal first tries to discover whether or not there is a warrant and then whether there is a tap without a warrant two things will happen. First, the tap will be taken off and secondly, the Minister will be told [by his civil servants] that there is not a warrant. That is the wrong way round. The first duty of the Tribunal should be to determine whether the line is intercepted. Its second duty is to determine whether there is a warrant."[20]

The main deficiencies of the current oversight system have already been touched upon. What we wish to emphasise is that new technology is simply incompatible with the ingenious but fatigued machinery devised fifteen years ago.

The impossibility of implementing key-escrow eluded the Government, not only because of poor lines of technical communication, but because it did not understand the culture of the Internet,

[19] suggested by Conservative MP, R. Shepherd *HC Debs col 245*, 16 January 1989, quoted in Birkinshaw 1996, p.48

[20] *House of Commons Hansard,* 12 March 1985, col 211-2

which in its own way is as powerful a force as economic globalisation, with its own internal logic of development.

Government proposals for decryption warrants appear to the Internet community as unworkable today as escrow did three years ago. The Internet won't change – Government will, and government should. There is a huge opportunity to enact reforms long enjoyed by other European and commonwealth democracies - it may also be the only effective catalyst to reform Agencies with diminishing morale and effectiveness.

- notification of targets of interception or surveillance (subject to evidence of prejudice to ongoing investigations)
- parliamentary scrutiny of security and intelligence affairs by a full select committee (with members nominated by party subject to security vetting)
- a surveillance complaints body which can hear arguments on proportionality
- a uniform system of judicial warrants for search, surveillance, and interception
- a Freedom of Information Act worthy of its name, to replace OSA

COMMUNICATIONS DATA – [CHAPTER 10.]

The proposal to put access to communications data on a statutory basis is long overdue, but on examination it appears that the proposal merely abolishes existing Data Protection safeguards on access, whilst relying on present oversight and complaint mechanisms with swingeing Executive exemptions.

We are not sure the extent to which the draftsmen of these proposals have official clearance for understanding existing COMINT agency capabilities for traffic analysis (who-is-talking-to-whom). At the "Scrambling for Safety" conference on March 23rd 1999, the officials who gave the first public presentation of Home Office policy seemed interested and perhaps surprised at the sneak preview of the "Interception Capabilities 2000"[21] report.

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.

[21] http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm

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, politically that is a terrifying prospect.

Under current IOCA, GCHQ "trawling warrants" specify a logical circuit or domain of capture, rather than topic or person. The idea is that signals are hoovered up, untouched by human hands, and then automatically selected by computer against a "certificate" issued by the Secretary of State which 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". In the age of plentifully cheap storage and supercomputers, it's unlikely that much needs to be thrown away. Technically and legally there is little to prevent harvesting the domestic Internet backbone in the same way that satellites and international cables are currently vacuumed, other than a stipulation that the targets for such interception should be persons outside the United Kingdom.

> "Personal data are exempt from the data protection principles, from the provisions of Parts II, III and V (rights of data subjects, notification by data controllers and enforcement) and from s 55 (the offence of unlawful obtaining for personal data) if the exemption is required for the purposes of safeguarding national security. A Minister will sign a certificate saying that the exemption applies, or at the time was required, and this is to be taken as conclusive evidence of that fact (s 28(2)). National security is not defined."[22]

Appeals to the Data Protection Tribunal against the issuing of a certificate are possible, however the tribunal is then constituted of three specially designated appointees of the Lord Chancellor, and the usual requirement for an equal number of representatives of the interests of data subjects and data controllers, is waived.

> "….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."[23]

---

[22] p.46, *Data Protection: The New Law*, Susan Singleton, Jordans 1998

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