# CLOSED CIRCUIT TELEVISION FOR INSIDE YOUR HEAD: BLANKET TRAFFIC DATA RETENTION AND THE EMERGENCY ANTI-TERRORISM LEGISLATION

*Caspar Bowden, Director of the Foundation for Information Policy Research (FIPR), explains the technical and legal context of unprecedented new surveillance capabilities, with particular reference to the UK's Regulation of Investigatory Powers (RIP) Act 2000. He discusses why these powers are unlikely to be effective in detecting or disrupting the communications of terrorist cells or organized crime, but present significant new threats to the security, privacy, and freedom of expression of the law-abiding.*

*{This article appeared in the Computer and Telecommunications Law Review, March 2002}*

At the time of writing, Part 11 of the UK Anti-Terrorism Crime and Security Bill (ATCS) will allow automated surveillance of the private lives of a substantial proportion of the population through analyzing the pattern of their electronic communications. The powers are deliberately broad, and can be exercised quite generally for non-terrorist as well as terrorist investigations. In short, it permits:

- ***Traffic Analysis*** ~ computerized "trawling" of who people talk to (by phone or e-mail), where they go (pinpoint tracking via mobile phones), what they read (websites browsed).
- ***Blanket data retention*** ~ Internet and telephone companies will be required to stockpile such data on the entire population for long periods—the penultimate step towards a national "traffic data warehouse," sought jointly by police, customs, intelligence and security agencies.
- ***Mass-surveillance*** ~ a police Superintendent or equivalent rank can authorize access to data on a single person or millions of people, without any judicial or executive warrant, and with no guidance on proportionality. Data thus obtained can be accumulated centrally and exploited speculatively.
- ***Public order, minor offences, health and safety, and tax*** ~ are valid purposes for the exercise of these powers, as well as counter-terrorism. The Home Secretary has now repudiated an assurance he gave that the new powers will apply only in terrorist cases.

Under the RIP Act, law enforcement already has extensive powers to intercept communications carried by telephone and Internet companies. The new proposals in ATCS can compel telephone and Internet companies to stockpile ***traffic data*** on all their customers in case they are required to provide information retrospectively to law enforcement.[1]

---

[1] *See* Home Office Press Release, *Blunkett Outlines Further Anti-Terrorist Measures*, *available at* http://wood.ccta.gov.uk/homeoffice/hopress.nsf/50e2456405b67f7d802566b3006819dc/2a5fc6811dec4c7180256ae6004fa4d3?OpenDocument (page updated Oct. 15, 2001).

Traffic data constitutes a near complete map of private life: whom everyone talks to (by e-mail and phone), where everyone goes (mobile phone location co-ordinates), and what everyone reads online (websites browsed). At present, the geographic coordinates of a mobile phone can be tracked to within a few hundred meters whilst the phone is switched on. The new 3G (third generation) phones will pinpoint location to a few meters,[2] and some operators have factored in revenue models that make use of this data commercially.

Currently, traffic data is logged in computer files and is either deleted or backed-up to magnetic tape periodically. There is usually no commercial need to refer to Internet logs more than a month old. For marketing or system performance research purposes, samples of anonymised data should suffice. As an illustration of the capacity of modern mass-storage systems, the web browsing behaviour of a million customers for a year could be held on about a hundred matchbox-size tapes. (Very large databases used by intelligence agencies can provide instant access to at least a thousand times this amount of data).[3]

Service providers typically do not handle traffic data logs securely, but even if that were the case, it is important to understand that traffic data cannot prove the identity of the author of an e-mail or the person who actually made a particular call. There is thus an inherent asymmetry in their usefulness in testing alibis. No amount of traffic data by itself can prove an alibi, because while it might be persuasive circumstantially, it does not eliminate the possibility that a bogus trail has been carefully laid by an accomplice. However the non-existence of a call record or an e-mail log could in theory disprove a claimed alibi. In practice, traffic data is admissible as evidence,[4] but it may be incomplete because of the system errors and failures which are rife on ordinary computers. It may be inaccurate, if for example, it has been "hacked" or corrupted in some way, and it may be sensitive, for example, geographic locations or websites implicitly revealing medical, political, sexual, religious matters. Data protection law gives full rights for subjects to access identifiable data collected about them. How will this legislation work if the proposed Bill becomes law?

On the economic front, the Internet Service Provider (ISP) business is increasingly commoditised. The extra costs arising from data retention and other surveillance measures that ISPs may be required to implement if the Bill becomes law could increase overheads to the point where cheap transatlantic bandwidth makes it attractive to locate or relocate servers in offshore subsidiaries where the legal and regulatory requirements are less onerous.

Even within Europe, different companies log widely different amounts and types of data depending on their business model, and some may already be in breach[5] of current European law requiring destruction of records irrelevant to billing or fraud control,[6] although national security exemptions[7] could be invoked to allow

---

[2] Pinpointing a 3G phone user can be performed using software which analyses signal timing. Pinpointing need not use satellite GPS, as is often misreported.

[3] *See Toward Petabyte On-Line Storage*, HPCWIRE (May 30, 1997) *at* http://www.tgc.com/hpcwire.html.

[4] *See* Peter Sommer's upcoming article, *Downloads, Logs and Captures: Evidence in Cyberspace*, 2002 COMPUTER AND TELECOMM. L. REV. issue 2.

5 *See* Stuart Miller & Paul Kelso, *Liberties Fear Over Mobile Phone Details, - Records Which Map Out Users' Whereabouts Held Indefinitely*, THE GUARDIAN, (Oct. 27, 2001), *available at* http://www.guardian.co.uk/uk_news/story/0,3604,581735,00.html.

6 Letter from Iain Bourne, Office of the Information Commissioner, to FIPR and Internet Service Providers Association (July 19, 2001).

data to be lawfully retained. In the UK, the RIP Act allows interception of the **contents** of communications only for national security, safeguarding economic well-being, and serious crime.[8] Any ISP can be required to install a "black-box" capable of relaying intercepts back to a central monitoring facility in the MI5 building ('NTAC'). Under great pressure during the RIP debate, the government eventually confirmed that the RIP Act confers **new powers to scan the contents of all the data** carried by an ISP.[9] This fact is not yet widely appreciated by ISPs or the legal community.

The RIP Act also allows access to traffic data, but for much broader reasons than for interception, including public order, minor crime, health and safety and tax. Both content and traffic data can lawfully be collected by the black-boxes directly, without serving the content warrant or traffic notice on the ISP.

A single Interception Commissioner has sole responsibility for oversight, checking over a thousand warrants issued by Secretaries of State – principally the Home and Foreign Secretary – and writes a brief annual report. Next year, he will also have to review tens of thousands of forms which various agencies will use to authorize themselves to access traffic data and account details. RIP empowers a Superintendent or equivalent rank to obtain **any and all** traffic data ISPs hold about groups or individuals. The proportionality of a request is supposed to be judged by the police and security agencies themselves, but no criteria or framework is provided in the Code of Practice to decide what is justified. For example, does a murder justify obtaining traffic data on fifty people or five thousand? What about a shoplifting offence? Or an anti-globalization protest? Or September 11th? There is no published guidance whatsoever, and since the powers are exercised in secret without judicial approval, it is difficult to see how any consistency will be achieved.

Under current data protection guidelines, once lawfully obtained under RIP, traffic data can probably be kept in police or intelligence databases for at least three years, and potentially indefinitely. Such processing is exempt from some or all of the data protection principles,[10] and there is no barrier to all such data being accreted into a single database for speculative purposes – somewhat analogous to the creeping enlargement of the national DNA database.

The new Interception Commissioner's first report was published in October 2001.[11] It makes no mention of the Internet, and there are no indications of how statistically robust sampling to investigate the vast number of cases, for widely differing amounts of data, will be carried out. The Home Office will not say when

---

7 *See* The Telecommunications Data Protection Directive (1997) § 32, *available at* http://www.hmso.gov.uk/si/si1999/19992093.htm (entered into force March 1, 2000).
8 *See* Regulation of Investigatory Powers Act (2000), Part 1, Chapter 2, § 22, *available at* http://www.hmso.gov.uk/acts/acts2000/00023--c.htm#22 (prepared Dec. 8, 2000). (This Chapter is not yet in force and the consultation on its Code of Practice, http://www.homeoffice.gov.uk/ripa/consultintro.htm, closed on November 2, 2001).
9 *See* Letter from Lord Bassam to Lord Phillips (July 4, 2000), *available at* http://www.fipr.org/rip/Bassam reply to Phillips on S.15.3.htm.
10 *See* Data Protection Act (1998) § 28-29, *available at* http://www.hmso.gov.uk/acts/acts1998/80029--l.htm (prepared July 24, 1998).
11 *See* Report of the Interception of Communications Commissioner for 2000, *available at* http://www.cabinet-office.gov.uk/intelligence/76463-COI-Rprt-InterComm.pdf (Oct. 31, 2001).

the Commissioner will be provided with promised "reliable and verifiable technical means"[12] to inspect the operation of black-boxes (which could be under remote control from NTAC), and proposes he should scrutinize exercise of traffic data powers by touring at least fifty locations around the UK to inspect paper records. There will not be any consolidated database of records to work from. Last year the RIP Tribunal, which is supposed to safeguard civil liberties, was criticized by the parliamentary watchdog, which said it "did not have sufficient secretariat to enable it even to open the mail, let alone process and investigate complaints."[13]

FIPR has previously drawn attention to the dangers of large-scale traffic-analysis, and proposes the following solution. A new type of ***data preservation*** order, judicially authorised case-by-case, could require ISPs to perform detailed logging and preservation of specific traffic data on specified targets, only for the same purposes as interception. As with intercepted content, FIPR believes that bulk traffic should be destroyed at the end of an investigation, or in finite time, with any exemptions subject to strict tests by an independent arbiter.

UK law enforcement agencies might be expected to support proposals for data preservation, but they are holding out for blanket retention with open-ended definitions. Ironically, UK law may need to provide extended data preservation powers in any case once the Council of Europe Convention on Cybercrime is implemented. The RIP Act does not obligate companies to record any data at all.

Some data already widely held is useful for investigations (start/stop of Internet sessions and phone logs), but we believe the line should be firmly drawn rejecting blanket retention of the online contacts and interests, and physical movements of the entire population. Automated trawling of traffic databases is a powerful form of mass-surveillance over the associations and relationships that constitute private life. It also reveals the sequence and pattern of thought of individuals using the Internet – it could be described as closed circuit television for the inside of your head. FIPR believes this is incompatible with the Human Rights Act (infringing Articles 8, 10, and 11 of ECHR) and undermines the basic rights and freedoms of a democratic society. The Information Commissioner has characterized even the notion of blanket data retention (let alone computerized analysis) as "disproportionate general surveillance."

The horrifying events of September 11th clearly weigh heavily in any scale of proportionality, and the Convention rights recognize limitations imposed by "pressing social need" for measures "necessary in a democratic society." Any human rights assessment of laws ostensibly justified on the grounds of combating terrorism therefore needs to take into account the likely effectiveness of such measures. It is far less persuasive to argue that some counter-terrorist benefit may be obtained from highly intrusive general surveillance of large parts of the population, than if the methods were effective against the terrorists themselves.

Yet it is a singular fact that surveillance via ISP and telephone traffic data can easily be evaded by using pre-paid (or stolen) mobile phones and web-based e-mail from public terminals to avoid identification. Organized criminals already routinely use the former, and reports of the modus operandi of the 9/11 terrorists indicate they used the latter. Web-based e-mail services can be provided via any website and will leave no trace

---

[12] *See* Lords' Hansard, RIP Committee Stage June 19, 2000: Column 14 – Amendment 50A, withdrawn after accepted in spirit, *available at* http://www.fipr.org/rip/parliament.html (last visited March 29, 2002).
13 *See* Intelligence and Security Committee Interim Report 2000-2001, *available at* http://www.official-documents.co.uk/document/cm51/5126/5126.htm (March 29, 2001).

with the ISP. They can be set-up on any computer with an always-on connection (domestic broadband is ideal), and there are thousands of examples large and small. Logically, therefore, the measures in the ATCS Bill measures will be ineffective in detecting or even inhibiting actual terrorist communications unless the power to compel logging and retention extends beyond ISPs and telephone companies to include:

- Any ISPs operating a web-cache logging the detailed browsing behaviour of their users in vastly greater detail than at present is lawful or required for business purposes.
- Commercial or free websites offering a web-proxy or anonymised web-browsing, authentication of e-commerce transactions, or web-based e-mail.
- Home computers running "peer-to-peer" file-sharing or communications applications. These logs could also be subpoenaed in Napster-style copyright cases, and summarily "extradited" under the sweeping terms of the new Council of Europe Cybercrime Convention.

This isn't fantastical. In fact, the wording of ATCS does not limit the powers of compulsion to "public" services; so all this will be possible if the bill passes unamended (the House of Lords were debating this at the time of writing).

Even such drastic measures would not eliminate possibilities for undetectable communication. The stealthy techniques of ***steganography*** (information hiding) allow messages to be camouflaged in sound, pictures, or other routine content in ways analogous to hiding a pebble on a shingle beach. It can be demonstrated mathematically that "the steganographer will always get through" (undetected) if sufficient care is taken. This is a bleak message for law enforcement, and the only solution is to "attack the platform" – if the computer sending or receiving the message can be found, it can be bugged in hardware or software. This approach is more palatable from a civil liberties point of view, because there is a built-in incentive to minimize its use, to minimize the risk of discovery.

If counter-terrorism is not the primary motivation for data retention, what is? Last year, a report by the National Criminal Intelligence Service (NCIS) was leaked to The Observer newspaper. It called on the Home Office to pass just such a law as is contained in ATCS, and further proposed the creation of a national *"traffic data warehouse"* covering the entire population. One year of records would be kept online in an enormous database, and at least three years held in archive. Government has declined requests to publish the 30-page submission, but a full copy is available on the web.[14] The document was remarkable in that MI5, MI6, GCHQ, ACPO, and Customs and Excise were prominently named as jointly supporting these ideas.

NCIS has been guilty of serial spin-doctoring. At the same time they were lobbying in secret to warehouse the entire population's traffic data, the Director of NCIS wrote that "conspiracy theorists must not be allowed to get away with the ridiculous notion that law enforcement would or even could monitor all emails."15

---

14 *See* Roger Gaspar, *Looking to the Future: Clarity on Communications Data Retention Law*, *available at* http://cryptome.org/ncis-carnivore.htm (Aug. 21, 2000).

15 Letter from John Abbott, Director General, National Criminal Intelligence Service, to GUARDIAN (June 15, 2000), *available at* http://www.guardianunlimited.co.uk/Archive/Article/0,4273,4029468,00.html.

NCIS has also briefed tabloids inaccurately on the effect of EU privacy directives, and were the driving force behind the key-escrow proposals abandoned in 1999.

Before ATCS was published, the Home Secretary seemingly gave a guarantee that extra traffic data obtained under new arrangements would be used " … strictly in the case of a criminal investigation against suspected terrorists."[16] But this was soon repudiated by the Home Office.[17] In fact, RIP provides a mechanism to impose just such a restriction to counter-terrorist purposes (an order under s.25.3.b), but there is no sign of any intention to do so. In the Supplemental Regulatory Impact Assessment,[18] the Home Office for the first time endorses blanket data retention on the entire population, but does not acknowledge that any new risks or concerns might arise. This contrasts with three Ministerial assurances given before the 2001 general election that the government would **not** introduce blanket retention, one of which was given in a Guardian Online internet Q&A session during the campaign![19]

What conclusions can be drawn from all this? Firstly, that a succession of Ministers have probably been misled about the true ambitions of law enforcement and intelligence agencies. Secondly, those agencies have varied motives and competence but have lobbied government collectively and in secret – their arguments are therefore untested by independent experts. Thirdly, that although these methods in themselves constitute new and significant dangers to civil liberties and democratic society, current oversight mechanisms have virtually no chance of detecting or deterring serious abuse at whatever level. Finally, that RIP and the associated powers in the ATCS are ripe for challenge under existing ECHR jurisprudence, but cases involving computerized traffic analysis will likely raise intriguing new arguments about proportionality, which impinge on several Convention rights.

***Author: Caspar Bowden***[20]

---

[16] David Blunkett, *Democracy Must Be Vigorously Defended*, TRIBUNE, Oct. 26, 2001. "…[W]e do need – **strictly** in the case of a criminal investigation against suspected **terrorists** – to have access to more information than we have at present. That is why we are working with companies on a code of practice with the result that they will keep billing records for longer than at present, to allow access in relation to **anti-terrorist activity**."

[17] *See* e-mail(s) from Rachel James, mailto:Rachel.James@homeoffice.gsi.gov.uk (Nov. 11, 2001) (in reply to question from FIPR dated Oct. 27, 2001).

[18] *See* Home Office, *Retention of Communications Data*, para.8, *available at* http://www.homeoffice.gov.uk/oicd/antiterrorism/retention_of_communications_data.pdf (last visited Feb. 20, 2002).

[19] *See* Labour e-minister Patricia Hewitt online, *available at* http://politicstalk.guardian.co.uk/WebX?128@112.hdYgcfAY4Xe%5e0@.ee82d04 (May 11, 2001); *see also* Patricia Hewitt and Charles Clarke, Joint Letter to Independent on Sunday (Jan. 28, 2001); *see also* Evidence of Patricia Hewitt (Minister for E-Commerce) Before Trade and Industry Select Committee (Dec. 13, 2000), *available at* http://www.parliament.the-stationery-office.co.uk/pa/cm200001/cmselect/cmtrdind/66/1121306.htm.

20 Caspar Bowden is Director of the Foundation for Information Policy Research (FIPR). FIPR (http://www.fipr.org) is a non-profit think-tank for Internet policy in the UK and Europe. Research topics include: legislation and regulation of electronic commerce and infrastructure, consumer protection, data protection and privacy, copyright, law enforcement and national security, evidence and archiving, electronic government and interaction with business and the citizen, and social inclusion. Donors have no influence over general or specific policy, which is governed by an independent Board of Trustees in consultation with an expert Advisory Council.