EUROPEAN PARLIAMENT

TEMPORARY COMMITTEE ON THE ECHELON INTERCEPTION SYSTEM

DIRECTORATE-GENERAL FOR COMMITTEES AND DELEGATIONS

BRUSSELS MEETING, 22-23 JANUARY 2001

INTERCEPTION CAPABILITIES - IMPACT AND EXPLOITATION

Paper 3

COMINT, privacy and human rights

COMINT, PRIVACY AND HUMAN RIGHTS

PRIVACY AND INTERNATIONAL TELECOMMUNICATIONS

1. During the 1980s, staff and visitors who entered the operations block, Building 600, of RAF Chicksands – a USAF listening station in England - would pass a turnstile and a security badge check to be confronted directly with a Sigint in-joke. Pasted to the wall was a copy of the International Telecommunications Convention. The Convention, which both the United Kingdom and the United States have ratified, promises that member states will protect the privacy of communications. Passing by, the operators set out to do the opposite.

2. This satirical presentation of the telecommunications treaty raises the abiding conundrum of intelligence oversight - that intelligence involves *ipso facto* breaking laws. Since the 1970s, former NSA staff who have talked about their work have often said that they were taught that secrecy was necessary because "Sigint is illegal". The increasing publicity and attention to this issue has raised the question of the general right to international telecommunications privacy, and how it may be enforced. Sigint, which comprehensively attacks the privacy of such communications, remains – unlike domestic wiretapping in most countries – unregulated and beyond the reach of most national jurisdictions.

3. Two international treaties protect international communications. The first is the International Telecommunications Convention (ITC), which sets up the International Telecommunications Union, based in Geneva. It and its subsidiaries are the governing bodies of international communications. Article 22 of ITC says

Secrecy of Telecommunications

> 1. Members agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.
>
> 2. Nevertheless, they reserve the right to communication such correspondence to the competent authorities in order to ensure the application of their internal laws or the execution of international conventions to which they are parties

4. The caveat on the undertaking of secrecy in communications relates only to "internal laws" of states. The Sigint arrangements between the UK, others and U.S. are not an "international convention". The convention appears only to authorize law enforcement undertaken for the proper purposes of law enforcement.

5. The Vienna Convention on Diplomatic Relations (1961) affects only governments, but is more specific: Article 27 says:

> *1. The receiving State shall permit and protect free communication on the part of the mission for all official purposes. In communicating with the Government and the other missions and consulates of the sending State, wherever situated, the mission may employ all appropriate means, including diplomatic couriers and messages in code or*

cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State.

2. The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions.

Article 30 specifies:

1. The private residence of a diplomatic agent shall enjoy the same inviolability and protection as the premises of the mission.

2. His papers, correspondence and, except as provided in paragraph 3 of Article 31, his property, shall likewise enjoy inviolability

6. The Universal Declaration of Human Rights, to which all UKUSA nations are signatories, specifies at Article 12 that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The same language is reflected in Article 8 of the European Convention on Human Rights which sets out the same position, with some qualifications:

1.Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Fourth Amendment to the U.S. Constitution stipulates:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

7. Each of these provisions is challenged by the activities described previously. When the U.S. Bill of Rights was written, it was inconceivable that the British soldiers who had been beaten back to their homeland could intrude on the privacy of an American household. The situation has changed, and with it the question of why privacy in communications should end at national boundaries.

8. Within Europe, these issues are being addressed in the context of growing federal and police collaborative arrangements which will shortly permit cross-border interception arrangements to deal with law enforcement activities against serious crime, narcotics trafficking, of terrorism. The availability of these new arrangements reduces or removes the need for intelligence agencies to conduct Sigint, if collaborative and effective law enforcement arrangements are in

place. According to the resolution drafted in 2000 in the European Parliament, all international interceptions must:

> *have a legal basis, be in the public interest and be strictly limited to the achievement of the intended objective; and*
>
> *even in the case of the fight against cross-border crime, adequate safeguards governing interceptions should be drawn up; and*
>
> *any form of interception by a Member State should be notified to the Member States on whose territory the persons whose communications are being intercepted are present.*

An accompanying resolution asserts "on a world-wide scale, the rise of the information society has not been accompanied by a corresponding revision of provisions on data protection". In relation to arbitrary searches or unreasonable search and seizure, it says:

> *any form of systematic interception cannot be regarded as consistent with that principle, even if the intended aim is to fight against international crime [and] …*
>
> *any Member State operating such a system should cease to use it.*

9. The duty to protect the privacy of international communications needs to be enhanced. Although existing national and international law is adequate in principle, what is required is building upon existing provisions to extend these instruments and conventions and their effects. Given new international collaborative arrangements for law enforcement, the conflict between Sigint activities and human rights could reduce as its proper remit became more restricted, to specific military and much more narrowly drawn national security purposes.

Privacy and human rights in UKUSA nations

10. During the U.S. Senate hearings in 1977, the alliance between Sigint agencies under the UKUSA agreement was cited as one reason why U.S. citizens traveling abroad should not enjoy the same protection as at home. On 19 July 1977, U.S. Attorney General Griffin Bell told the Senate Select Committee on Intelligence that his reasons for taking this position:

> could only be discussed in executive session … many of the problems arise out of the fact that overseas there is a fair degree of co-operation between our Government and the police and intelligence services of other nations[1]

11. Why this should be so was not explained, nor is any explanation obvious save a desire to keep concealed the extensive interlinking and collaboration taking place within the international Sigint network.

12. At the time, none of UKUSA nations had given their citizens any protection, nor had they apparently considered it necessary to do so. Sigint everywhere operated in a realm of its own, where history has shown legality or human rights not to be a significant consideration.

---

[1] Hearings before the Subcommittee on Intelligence and the Rights of Americans of the Senate Select Committee on Intelligence, on S.1566, p17, 19 July 1977.

13. The changes that started in the U.S. spread. In the UK, a complaint about a wiretapping case brought under the European Convention forced the UK government to introduce an Interception of Communications Act in 1984, placing statutory controls over wiretapping and requiring a non-judicial warrant, signed by a Secretary of State, before domestic interceptions could proceed. But the interception of international calls was authorized under a different procedure. In this case, warrants did not name targets but identified groups of communications links, which could be intercepted as a whole.

14. Once intercepted, GCHQ was authorized automatically to extract "classes" of communications described in certificate issued alongside the warrant. These provisions were precisely matched to the technology of the Dictionary.

15. The certificates described the targets of communications interception about which the British government wished Sigint reporting. According to the law, the certificates should not include specific named persons. But their names could of course be included in the filtering selection databases within the Dictionary. Although the UK does not have an equivalent of the Fourth Amendment, this maneuver prevented even the limited challenges that citizens might bring before an Interception of Communications Tribunal to complain about domestic wiretapping. The law stipulated that a person could only complain about international interception if they were specifically identified in the certificate – but not in the contents of the Dictionary. According to former members of the British Security Service (MI5), no high-level or legal checks were needed on the names that might be added to GCHQ's Dictionary target lists in this way.

16. The controversy over Echelon led both Australian and Canadian authorities to issue statements acknowledging for the first time their participation in the UKUSA alliance and describing their policies on Sigint and privacy. Australia has an Inspector General of Security and Intelligence with powers to examine the conduct and operations of its Sigint organization, DSD. Canada appointed attorneys to work inside its Sigint organization in 1986. In 1997, a Commissioner was appointed to oversee its Communications Security Establishment (CSE). NSA has an Inspector General, as well a substantial number of legal counsel, including some working in its operations division. Britain and New Zealand have not made provisions of this kind.

17. According to the Director of Australia's DSD[2], "to ensure that [our] activities do not impinge on the privacy of Australians, DSD operates under a detailed classified directive approved by Cabinet and known as the "Rules on SIGINT and Australian Persons". The directive is said to prohibit the deliberate interception of communications between Australians in Australia, the dissemination of information on Australians gained accidentally during the course of routine collection on foreign communications, and the reporting or recording of the names of Australians mentioned in foreign communications.

18. There are exceptions. The Cabinet directive specifies that Australians' international phone calls, faxes or e-mails can be monitored by DSD in specified circumstances. These are stated to include "the commission of a serious criminal offence; a threat to the life or safety of an Australian; or where an Australian is acting as the agent of a foreign power". The Director of DSD must give specific approval in each case. The interception of domestic calls in Australia is restricted to the police and ASIO, the Australian Security Intelligence Organization. As

[2] Statement by DSD Director Martin Brady, broadcast on the *Sunday Programme*, Channel 9 TV (Australia), 11 April 1999.

described, the Australian procedures appear similar to U.S. procedures, while not having any force of law.

19. Although Australian journalists have applied for this document under freedom of information laws, it has not yet been released in whole or in part. The Inspector-General of Security and Intelligence, who can receive complaints and conduct inquiries, monitors compliance with the directive. The DSD Director, Martin Brady also claimed that other UKUSA nations followed common procedures with Australia. "Both DSD and its counterparts operate internal procedures to satisfy themselves that their national interests and policies are respected by the others". The Australian position is that if NSA or another agency intercepts Australian traffic and reports a message from an Australian citizen or company whom DSD has decided to leave alone, they are supposed to strike out the name and insert "Australian national" or "Australian corporation" instead. If DSD has authorized the targeting of that person, the opposite applies.

20. According to Hager,[3] and also GCHQ sources, Sigint reporters and analysts in New Zealand and Britain are told to follow U.S. minimization rules when dealing with U.S. nationals. Thus, they are asked to replace specific names with standard generic phrases such as "U.S. person".

21. In his 1997-1998 report, the Commissioner of the Canadian Communications Security Establishment suggested for the first time that such policies were in force across UKUSA, and that one agency would follow the policy of the other in dealing with UKUSA nationals. According to his report, CSE has committed to "respect the corresponding procedures of its close and long-standing allies":

22. CSE undertakes explicitly to treat the communications of Second Party nationals in a manner consistent with the provisions issued by the agency of that country, provided such procedures do not contravene the laws of Canada. This is a reciprocal undertaking to ensure that the Second Parties do not target each other's communications or circumvent their own legislation by targeting communications at each others' behest. In other words, they do not do indirectly what would be unlawful for them to do directly".[4]

23. If this statement is generally true, then it demonstrates that countries co-operating in policing and intelligence can operate with and agree to protect human rights outside their own borders. The value of this assurance is limited by the fact that the agreement to do this has never been published, or referred to by any government; that only Canada has ever suggested that there is an agreement; and that the protections, if valid, extend only as far as the "Second Party" country's own rules for the privacy of its citizens. These rules are substantially classified in the US, and wholly unavailable elsewhere. They do not exist in the UK.

24. The technical arrangements for the global network also indicate that the restriction on disseminating U.S. identities (etc) is limited to the collective outside boundary of the UKUSA Sigint organizations. The information passed from country to country by Dictionaries is raw, unprocessed traffic, not end product reports. No restriction affects the transmission of raw data from country to country.

January 2001

[3] Secret Power, *op cit.*
[4] Annual Report of the Communications Security Establishment Commissioner, Ministry of Public Works and Government Services, Ottawa, Canada, 1998.