Duncan Campbell—written evidence (IPB0069)

My name is Duncan Campbell. I am an investigative journalist and a registered court expert witness on communications and computer data.

I write to offer evidence and to give oral evidence if requested to your Committee on the Draft Investigatory Powers Bill proposals in areas of which I have specialist knowledge or experience.

I gave evidence[1] in October 2012 to the Joint Committee then reviewing the Draft Communications Data Bill, and on which the government did not proceed. Further and fuller details of my work and experience over the past 35 years are at the end to this note.

I would also offer to assist in supporting evidence to be provided to the Committee by Mr William Binney, formerly of the United States National Security Agency. I have worked with Mr Binney during the course or the last six months so as to assess and report on the applicability and relevance to the UK of technical methods and approaches developed while he was a Technical Director of the NSA, particularly in regard to minimising intrusion within lawful boundaries and consequently improving operational efficiency in respect of bulk collection.

These matters also have specific and direct relevance to the potential for the general protection of Parliamentarians' communications (and the communications of other protected professions, such as lawyers) from random and unlawful intrusions as a result of unconstrained bulk collection.

This is a matter on which I reported shortly before this Bill was introduced in November this year. The gist of my report was that the Investigatory Powers Tribunal had in 2015 been misled by the government side as to the practicality of restraining collection of MPs' and Peers' communications within the apparatus of bulk collection, [2] pursuant to the long-established Wilson doctrine.

I have studied and assessed extensive further material relevant to the contention that excess interception and overcollection has prejudiced security by drawing focus and resources from potential directed intelligence or human intelligence operations against identified suspects onto almost incomprehensibly large systems of general population surveillance.

There are abundant examples of this in many now published studies and reports of the U.S. National Security Agency, for which Mr Binney worked. Even as early as 2006, NSA colleagues reported that:

> "Everyone knows that **analysts have been drowning in a tsunami of intercept whose volume, velocity and variety can be overwhelming**."[3]

There are also examples of how directed or intrusive surveillance, as opposed to bulk collection, has been the primary means of detecting and preventing both terrorist activities and conspiracies to abuse children.

---

[1] www.parliament.uk/documents/joint-committees/communications-data/Oral-Evidence-Volume.pdf#page=301

[2] http://www.theregister.co.uk/2015/11/04/gchq_smart_collection_nsa_man_bill_binney

[3] https://www.eff.org/files/2015/05/26/20150505-intercept-sidtoday-tsunami-of-intercept-final.pdf (emphasis added)

I have more recently reported on the previously wholly secret aspects of the development over the last 15 years of general multiple mass linked databases on the entire population or sub-populations as a means of "enrichment" of communication data analyses. [4] Some of these have now been avowed, but the nature of most information has not been identified to the public or Parliament generally.

This includes the implications of the creation of a permanent national telephone call and Internet connection records database, held secretly by the government, and which was not avowed until the day this bill was presented in Parliament.

I have referred in my report to the role of the seldom-mentioned intelligence support agency NTAC (the National Technical Assistance Centre) in acquiring personal bulk information databases by overt and covert means, the majority of which remain undeclared and unjustified to Parliament, notwithstanding admissions that have been made.

A grave effect of this admission is that Parliament has been extensively and repeatedly misled over the past 15 years by statements which can now be seen to be inaccurate about the need for and unavailability of historical call data records. This has also to my knowledge prejudiced police investigations and prosecutions, as well as the proper defence of accused persons in serious criminal cases. In such cases, which may well have involved lengthy and repetitive police enquiries over many months before arrest, charge and trial, senior investigation officers and/or defendants' legal representatives have been told by telecommunications companies that data is not held and is destroyed after the retention period of up to one year.

It is now apparent that this was a charade, in that all communications data was collected, retained and analysed nationally in a process quite separate to the authority Parliament provided under RIPA.

Like many others who wish to assist the Committee, I have been impaired in being able to assess and consider the Bill's provisions and its implications for the next decade or more. It would be of immense assistance to mature and productive discussion, and to Members' scrutiny, if significantly more time were made available within the Parliamentary timetable I have watched as successive Bills at 15 year intervals have obfuscated or failed to address technological and legal issues. This is the largest bill ever, and has brought hitherto clandestine activity affecting every voter into the open. It merits careful reflection.

Noting the shortness of time and the Committee's timetable, I intent within that limit of time to provide further examples and assessments relevant to the questions the Committee has laid out.

Duncan Campbell

PERSONAL EXPERIENCE AND INVESTIGATIONS

Between 1976 and the present, I have identified and framed important issues concerned with communications intelligence and surveillance for Parliament and the public, and for the European and international communities.

I described and brought to general attention surveillance arrangements and facilities which successive British governments have planned and/or operated contrary to UK or international law,

[4] http://www.theregister.co.uk/2015/12/16/big_brother_born_ntac_gchq_mi5_mass_surveillance_data_slurping

and/or outwith law generally, and/or without due accountability to Parliament and the Courts. These reports have resulted in official investigations, judgments and legislative changes over three decades.

My reporting in 1980 led directly to the passing of the Interception of Communications Act 1985,[5] and to the creation of the offices of the Interception of Communications Commissioner and the Interception of Communications Tribunal.[6] His reporting in turn contributed to the passing of the Security Services Act 1989,[7] the Official Secrets Act 1989,[8] and the Intelligence Services Act 1994.[9] These brought the separate branches of the intelligence and security services within the remit of statute law and created formal mechanisms for accountability, including the formation of the Parliamentary Intelligence and Security Committee. The process continues to this day.

Since 1979, and in particular since 2002, I have worked as a forensic expert witness in major terrorism and other serious criminal cases in the Britain and Ireland In these cases, I has been employed to analyse, audit and report on large quantities of complex communications and computer data disclosed under the provisions of RIPA.

I have provided evidence concerning communication interception and communications data to the Court of Appeal,[10] the Supreme Court,[11] the Interception of Communications Tribunal, and the European Court of Human Rights, as well as to Crown and other UK Courts. The cases have included the use of communications data and communication interception evidence from overseas jurisdictions admitted in UK criminal proceedings.

In 1998, I was appointed a consultant to the Scientific and Technological Options Assessment (STOA) office of the European Parliament and asked to prepare a report on communications surveillance and communications security. The European Parliament published my report "Interception Capabilities 2000",[12] in April 1999.

In January 2001, I provided further reports on communications intelligence to the European Parliament Temporary Committee on the ECHELON interception system.[13] The committee made substantial recommendations to curb and restrict communications surveillance for the purposes of the protection of human rights and of European commerce. The recommendations were passed in their entirety by the European Parliament on 5 September 2001. [14]

From October 1999 to June 2000, I was a senior research fellow at the Electronic Privacy Information Center (EPIC), Washington DC. I there prepared a report intended for the United States Congress on the satellite communications interception arrangements known as "Echelon."[15]

---

5 1985, chapter 56.

6 *Ibid*, sections 7 and 8.

7 1989, chapter 5.

8 1989, chapter 6.

9 1994, chapter 6.

10 R v Winters [2008] EWCA Crim 2953; [2008] WLR (D) 387, R v Breton [2008] EWCA Crim 2935, Clifford v Herts [2008] EWHC 2549, Clifford v Herts [2008] EWHC 3154, R v Iqbal [2009] EWCA Crim 1627, Clifford v Herts [2009] EWCA Civ 397, Clifford v Herts [2009] EWCA Civ 1259.

11 R v Austin & ors, Supreme Court [2009] EWCA Crim 1527.

12 http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184(PAR01)_EN.pdf

13 http://home.datacomm.ch/lbernasconi/repository/texts/echelon.europa/7747.html, http://home.datacomm.ch/lbernasconi/repository/texts/echelon.europa/7752.html, http://www.europarl.europa.eu/meetdocs/committees/temp/20010322/433524EN.pdf

14 http://europa.eu/rapid/press-release_SPEECH-01-368_en.pdf?locale=en, http://www.european-security.com/index.php?id=784.

Between 1999 and 2002, I testified and provided reports on communications intelligence and interception to the national Parliaments of Denmark, Germany, Japan, the Netherlands, and Sweden and to the intelligence supervisory committee of the Belgian government.

I was instructed by Liberty and Keir Starmer QC (later the DPP and now MP), as the expert witness for the applicants in ICT hearings and the subsequent ECHR case on filtering and communications surveillance using bulk data, *Liberty v UK*. [16]

In its judgment issued in 2008, ECHR held that United Kingdom law did not provide "adequate protection against abuse of power" in respect of bulk data. The Court criticised the "very wide discretion conferred on the State" to intercept and examine bulk communications.

Although found in breach of Article 8 and ordered to pay damages, the United Kingdom government omitted to enact legislative changes on the basis that the Interception of Communications Act 1985 had been superseded by RIPA by the time of hearing and judgment. I am aware that the Committee's remit considers whether the breach of Article 8 will be remedied by the proposed Bill.

In May 2015, I was invited to open a conference on Intelligence, Security and Privacy held at Ditchley Park in conjunction with the new director of GCHQ, Mr Robert Hannigan.[17]

Further details of key issues and reports affecting communications data

The matters reported and briefly described below are material to issues which arise in the draft Investigatory Powers Bill, including compliance with privacy and other legislation, financial probity, the ability of citizens to understand and anticipate the effects of legislation, the role of filtering systems, and the concealment of projects and technical arrangements from Parliamentary oversight.

- GCHQ

  Issue – activities of the intelligence services unacknowledged to Parliament, unaccountable and operating outside the framework of statute law.

  In 1976, I and a co-author published the first article to describe the nature of communications surveillance activities conducted by Government Communications Headquarters (GCHQ). At the time GCHQ was not known to Parliament or the public, nor acknowledged as an intelligence agency, although it was, then as now, the largest of Britain's intelligence services. The "Eavesdroppers" report was controversial throughout the latter 1970s.[18]

---

15 See www.duncan.gn.apc.org/EPIC_2000.pdf .

16 Liberty, British Irish Rights Watch and the Irish Council for Civil Liberties ("Liberty and others") v the United Kingdom, 48 ECHR 1.

17 http://www.ditchley.co.uk/conferences/past-programme/2010-2019/2015/intelligence

18 "The Eavesdroppers", Time Out (London), 21 May 1976. See www.duncan.gn.apc.org/ Eavesdroppers_1976.pdf.

The publication led to internal reviews in which the Legal Adviser to the Foreign Office minuted *inter alia* that "it now seems clear that [the interception of foreign embassies' communications, as the article described] is at least a dubious practice."[19]

Subsequently, GCHQ's activities were formally acknowledged and placed under statutory supervision by the Intelligence Services Act 1994.

- Telephone tapping

  Issue - prior to 1985 telephone tapping (interception) in the UK was conducted without statutory legal authority and contrary to ECHR.

  In 1980, I published reports describing the scale and technical arrangements for telephone tapping activity in the United Kingdom.[20] The report led directly to a Home Office white paper instituting supervision arrangements for interception for the first time.[21]

  My 1980 reports, and his subsequent provision of technical evidence to the European Court of Human Rights on "printer metering" (the earliest form of communications data) in the case of *Malone* led to an ECHR judgment finding the United Kingdom in breach of Article 8. The Court found that UK law failed to 'indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities". [22] This is the historical antecedent to the contemporary and arguably no longer relevant split between content and metadata.

- Interception of commercial satellite communications *(Echelon)*

  Issue – from 1969 on, the United Kingdom created and participated in a clandestine program to intercept all commercial satellite telecommunications, including the communications of all UK private citizens and businesses, as well as those of allied countries.

  In 1987, I published a report describing the nature of international communications satellite surveillance activities conducted by GCHQ in collaboration with international partner agencies. The activity, known as "Echelon", has not been described or publicly acknowledged to Parliament.[23]

  The first known type of communications content and data filtering was developed for the Echelon project in 1969. The system initially used early computers to process and filter intercepted communications data using lists known as "Dictionaries". [24] These continue to be used to this day.

  Although extensively examined by the European Parliament and national Parliaments, the legality of the Echelon system and the role of Echelon dictionaries in filtering communications has not been tested before the ECHR or in other fora.

---

19 Sir Arthur Hockaday to D of HQ Sy, 27 June 1978, PRO file DEFE 47/34; cited in Richard G Aldrich, *GCHQ*, Harper Press 2012, pps 360 and 599.

20 See www.duncan.gn.apc.org/Interception_1980.pdf.

21 `The Interception of Communications in Great Britain', Cmnd 8191, March 1981.

22 Malone v United Kingdom (1984) 7 EHRR 14.

23 See www.duncan.gn.apc.org/Echelon_1988.pdf.

24 Aldrich, *op cit*, pps 342-344.

- Communication intelligence satellite constructed without parliamentary authority *(Zircon)*

  Issue – during the 1980s, GCHQ obtained ministerial authority to spend £500 million to acquire a proposed signals intelligence satellite without advising the Public Accounts Committee.[25]

  Notification had been required under a parliamentary agreement resulting from previous concealed overspending on the Polaris missile improvement program known as "Chevaline".[26]

  I reported on the satellite project, known as Zircon, for the BBC and in the press.[27] The BBC report was initially withheld on government request but was transmitted in 1988.

- Unlawful Interception of telecommunications *(Liberty v UK)*

  Issue – between 1990 and 1997 all communications to and from the Irish republic were intercepted and processes at a specially constructed facility in Cheshire, using "filtering" to extract content and data of interest.

  The normal arrangements for interception of communications in the period were that British Telecom would be served with a warrant under IOCA, and would make necessary technical arrangements. Exceptionally, the wholesale interception of all communications in Cheshire was carried out without BT co-operation in the normal way.

  The arrangements at the Cheshire facility (the "Capenhurst tower") involved obtaining the content and addresses of telephone calls, faxes and emails. These were stored and filtered before being transmitted to users by optical fibre cables.

  The operations at the Capenhurst tower were at the centre of the *Liberty v UK* case before ECHR, as described above. The Court found that the filtering procedures, described by government witnesses as "drawing down", did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. State interference with the applicants' rights under Article 8 was therefore found not to be "in accordance with the law".

Biographical

I graduated in physics from Oxford University in 1973 and further trained in Operations Research at the University of Sussex. I was a consultant on Telecommunications to the Technology Faculty of the Open University and in that capacity co-wrote a textbook on "The British Telephone System" for the University's Systems Behaviour course. I am a member of the Institute of Telecommunications Professionals (ITP) and a Fellow of the Royal Society of Arts. I am a visiting fellow and lecturer at the Media School of Bournemouth University.

---

25 See www.duncan.gn.apc.org/zircon_1987.pdf.

26 Ninth Report from the Public Accounts Committee, Session 1981-82, Chevaline Improvement to the Polaris Missile System, HC 269.

27 See www.duncan.gn.apc.org/zircon_1987.pdf.

21 December 2015