Draft Comms Data Bill – UKNOF 9/10/2012

Disclaimer: this is my distillation of 448 pages of detailed consultation responses. I've tried to produce a fair and balanced overview but there may be errors.

Trefor Davies

timico

Tuesday 10 July

- Charles Farr OBE, Director of the Office for Security and Counter-Terrorism
- Richard Alcock, Director of Communications Capability Directorate,
- Peter Hill, Head of Unit for Pursue Policy and Strategy Unit, Home Office

Wednesday 11 July

- David Davis MP
- Nick Pickles, Director, Big Brother Watch
- Jim Killock, Executive Director, Open Rights Group
- Dr. Gus Hosein, Executive Director, Privacy International

Thursday 12 July

- Panel 1:
- Donald Toon, Director of Criminal Investigation, HMRC
- Cressida Dick, Assistant Commissioner, Metropolitan Police Service
- Gary Beautridge, Assistant Chief Constable, Association of Chief Police Officers
- Trevor Pearce, Director-General, Serious Organised Crime Agency
- Peter Davies, Chief Executive, Child Exploitation and Online Protection Agency

Thursday 12 July

- Panel 2:
- Daniel Thornton, Head of Enforcement Legal, FSA
- Councillor Paul Bettison, Leader of Bracknell Forest Council, LGA Regulatory Champion, and member of the LGA Safer Communities Board, Local Government Association
- Gillian McGregor, Director of Operational Intelligence, UKBA
- Nick Tofiluk, Director of Regulatory Operations, Gambling Commission

Tuesday 17 July

- Panel 1:
- Angela Patrick, Director of Human Rights Policy, Justice
- Rachel Robinson, Policy Officer, Liberty
- Jim Killock, Executive Director, Open Rights Group
- Nick Pickles, Director, Big Brother Watch

Tuesday 17 July

- Panel 2:
- Professor Anthony Glees, Director of the Centre for Security and Intelligence Studies (BUCSIS), University of Buckingham
- Dr Julian Richards, Co-Director of the Centre for Security and Intelligence Studies (BUCSIS), University of Buckingham

Tuesday 4 September

- Professor Peter Sommer, Visiting Professor, De Montfort University Cyber Security Centre
- Professor Ross Anderson, Professor of Security Engineering, University of Cambridge
- Professor Sadie Creese, University of Oxford
- Glyn Wintle, Chief Consultant, Firewolf

Wednesday 5 September

- Nicholas Lansman, Secretary General, Internet Services Providers' Association (ISPA)
- Malcolm Hutty, Head of Public Affairs, London Internet Exchange (LINX)
- Jimmy Wales

Summary of written submissions

- 447 pages
- 91 submissions
- 69 out and out opposed
- 7 concerns
- 10 for
- 3 supportive but with reservations
- 1 non-committal
- 1 unconvinced

Those for the bill

- HMRC - CD is a critical investigative and evidential tool…hinder our ability to identify and prosecute criminal gangs and individuals that attack the UK tax system
- SOCA's …it will ensure law enforcement can maintain access to subscriber data, traffic data and service data in very much the same manner as it currently does, but that the data retained by CSPs will reflect the changes in technology and thus include information relating to communications sent using the internet.
- UKBA believes that the Government has made a convincing case for the new powers. The harm caused to the UK through the smuggling of drugs, organised facilitation and trafficking cannot be overestimated.
- FSA - We welcome the draft Communications Data Bill, which would consolidate and update powers essential to our enforcement work

More For

- Sir Paul Kennedy IoCC - The current inspection regime works well and I regard it as robust. As such, I do not anticipate changing my current oversight regime in relation to the acquisition of communications data
- says existing model for safeguards will improve by excluding LA access

Local Government wants in

- LGA believes that the current framework through which councils can access communications data provides the safeguards that the public are looking for.
- NAFN - Local authorities acquire communications data lawfully for relevant statutory enforcement and use it effectively in the investigation and prosecution of a broad range of criminal offences including serious crime.

Telefonica UK

- The widening of the scope to include TUK's own customer's data that may not currently be held for business purposes *appears* to be a *reasonable* extension of today's powers. Widening the scope to ANY data that happens to traverse our network does not. TUK is currently not convinced that all providers of UK communications will be treated equally and fear that UK based providers may find themselves disadvantaged by this Bill.
- TUK does not believe the plans are at all robust. The spectrum of "overseas providers" goes from multi-national players who see the UK as a tiny percentage of their market and who will be unwilling to change their trading practices to suit, through to backroom application developers who will be impossible to locate.

Virgin

At this stage, our primary concern with the draft Bill as it stands relates to the retention requirements on providers not previously caught by data retention requirements and the requirement for UK providers to retain data of these providers. Virgin Media currently enjoys good working relationships with a range of third parties, both domestically and internationally. In many cases, Virgin Media makes their applications and services available to its customers through, for example its TiVo service. If Virgin Media is legally obliged to provide data from such third parties, this may well damage its commercial relationship with those parties and other third parties, particularly those based overseas who may be reluctant to make their services available to virgin media

Other concerns

- Law Society – weak evidence base
- Direct Mail Association – generally supportive doesn't want it to apply to the postal service
- ISPA – questions way costs are calculated & believes it is an extension of scope
- ADM Shine supportive but wants it restricted to gov't agencies only
- The Global Network Initiative – generally for in principle but thinks this is an opportunity to set the global standard

The Chartered Institute for IT

- “inconsistencies between purpose and proposal.”
- “The purpose stated by Theresa May is: “to protect public; bring offenders to justice by ensuring that communications data is available to the police/security/intelligence agencies”. However, she also notes that police, SOCA and HMRC already “have access to the full range of communications data.”
- If so it is not clear why further powers are needed. Later on it is said that communications data – regarding email and internet – is less available and harder to access.”

Twitter

- Most governmental entities, including the US, have exerted great pressure on companies to minimize the collection of user data rather than increase it.
- Wants users to be notified when data is provided about them
- If enforced in the UK it will reduce ability of CSPs to refuse same access to data in less democratic regimes
- If enforced on a UK company on overseas based traffic but info not passed on to host platform it could affect accountability to regulators in own country re privacy

Vodafone

- Responsibilities of UK and overseas providers
- Interaction with privacy regulation
- Retention and deletion requirements
- Definition of valid requesting authority
- Oversight
- Technical boundaries

Against the Bill

- JANET
- Just West Yorkshire
- Liberty
- LINX
- the Newspaper Society
- Open Rights Group
- Society of Editors
- Timico Ltd
- The Tor Project
- Wikimedia UK

Against con't

- Equality & Human Rights Commission
- The Coalition for a Digital Economy
- The Bar Council of England and Wales
- Privacy International
- Big Brother Watch
- JUSTICE
- The foundation for Information Policy Research

A few objectors' views ...

- Peter John - 6 people die every year falling out of trees. But there is no expectation that crash mats will be placed under all trees in the UK 'just in case'.
- Keith Edkins - "about as robust as a chocolate teapot"
- Giles Murchison – "Verily, how mighty is the Secretary of State, who can "ensure" anything in the ever-changing world of the internet: how mighty, rather, is the Queen in Parliament to be able to bestow this power."
- Wendy Cockcroft – "the proposed bill ... represents the venal, selfish, sleazy state of the of the Government who proposed it and is a blight on Britain's record as a free and fair (country)!"

BIG DISCLAIMER ON THIS ONE (TD)

- Has the Home Office made it clear what it hopes to achieve through the draft Bill?
- **Robert Smith -** No, the excuse fighting terrorists is rubbish. There's something that tends to identify terrorists, they are Muslims. The entire population of the UK is not Muslim (yet), ergo the correct decision would be to only monitor those belonging to that religious group. Of course, this government is as spineless and directionless as the last lot and can't be seen to be picking on any minority, preferring to obliterate any idea privacy for all of its citizens.

Paul Bernal

- render things like internet banking, ecommerce and VPNs untrustworthy.
- Peter Hustinx, the European Data Protection Supervisor, called the Data Retention Directive the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects
- the draft Bill is so broadly written it could even be used to monitor carrier pigeons.

Big Brother Watch

- Firstly, we would begin by reaffirming our view that the operation and oversight of the Regulation of Investigatory Powers Act is deeply flawed, and to add further legislation that is based upon this Act without first undertaking a comprehensive review of RIPA is negligent to the point of recklessness
- This Bill ends the presumption of innocence as we know it.
- The Home Office has recognised even if this project is 100% successful, it will still leave a capability gap of 15%.

Big Brother Watch – is RIPA working

- huge variations in the way Communications Data is accessed by police forces. eg, Kent Police officers in two years made 7664 requests for data, with 3237 of those rejected internally. In the same period Merseyside made approximately 30,000 requests with 500 rejected internally.
- Under RIPA (& this Bill), innocent person whose communications data is wrongly accessed couldn't seek redress as they would most likely never know what had taken place. Only10 people found to have been wrongfully surveyed from more than three million RIPA authorisations (5 pers in 1 family) it is impossible to say with any confidence that the Commissioner/Tribunal model of oversight is working or indeed fit for purpose.
- We support the view that law enforcement agencies should, like public authorities, require a warrant to access communications data.

Greg Callus

- … “significant disparities between police forces in the rates of rejection of RIPA requests by DPs, ranging from 0.19% to over 30%. “

More agin

- COADEC When conducting the Impact Assessment to support the Bill which determined the cost level announced, the Home Office only consulted users of the data.
- Human Rights Commission - Currently, based on the information presented, our analysis is that a case for the proposed measures has not been made.
- JANET - the possibility of many new processes for obtaining communications data will lead to confusion and create new opportunities for unauthorised access to that data

Comms Data vs Content

- Sir Paul Kennedy - communications data requests are significantly less intrusive than acquiring the content of communications.
- Tor Project - The reason that communications data can be more sensitive than content is that it is more amenable to automated analysis, particularly when collected in bulk (as proposed by the draft bill). Content is designed for humans to read, and it is a challenging problem for computers to accurately interpret content. In contrast, communications data is designed for computers to interpret and so is far easier for computers to analyse and allowing a more accurate and detailed profile of individuals to be built than is possible with current technology to interpret content.

Risk to UK business

- Projects, such as Tor, may also consider that carrying out software development in the UK is too high a risk, because of the possibility that this proposed bill could be used to compel a programmer to introduce a back-door into a program to collect communications data.

Data Security (Privacy International)

- ...risk caused to such information by human error, loss or theft. In January 2008, the MOD lost details of 600,000 persons interested in joining the UK Armed Forces by the MOD. In July 2008 news reports emerged that the MOD had admitted that 658 laptops had been stolen, 89 lost and 32 recovered since 2004 and 121 memory sticks were unaccounted for. Thirty five laptops were reported to have been lost at GCHQ resulting in concerns raised by the Intelligence and Security Committee in their 2007-2008 annual report. In the same year, a mobile telephone sold on eBay was found by the new owner to contain photographs and information relating to terrorism investigations which had not been the previous owner, an operative in MI6.

Lessons learnt from other countries?-PI

- The technology for the proposed scheme is primarily used in dictatorships. The details of such approaches and abuses tends only to emerge once these dictatorships are overthrown, for example, in the aftermath of the Arab Spring. Detailed evidence is now emerging revealing the technologies and techniques used by the previous Libyan government against its citizens, and some information about surveillance and censorship systems in Tunisia (which also edits email in transmission) and Egypt has also come to light.

wikimedia

- After studying the Bill we remain unclear as to whether our charity, Wikimedia UK, would be classed as a 'telecommunications operator'.
- We submit that in its current state the Bill is not fit for purpose... We would draw the attention of the Committee to the fact that the UK would be conspicuous by exception in the democratic world if this Bill was to be enacted. Evidence given to the Committee suggests that this extent of collection of data has only been implemented nationally in China, Iran and Kazakhstan and such national scale centralised level of data collection has not been done in a democratic country.