HOME OFFICE

Consultation Paper on a Code of Practice for Voluntary Retention of Communications Data (under the Anti-Terrorism, Crime and Security Act 2001

Published 11 September 2003

Response to the Consultation Paper

Introduction

In March 2003 the Home Office published a consultation paper on the issue of a code of practice under Part 11 of the Anti-Terrorism Crime and Security Act 2001 (www.homeoffice.gov.uk/inside/consults/closed/papers2003.html). The purpose of this paper was to seek views on a code of practice, which would allow communications service providers to retain voluntarily communications data for periods that may exceed their current business practices.

2. Following a twelve-week consultation period, a total of fifty-seven replies had been received. The spread of responses covered the industry, government bodies, law enforcement agencies, the legal profession, academia and the general public. This paper attempts to summarise the responses.

Summary of responses

3. The consultation paper asked five specific questions. Respondents did not restrict themselves to only these five questions but also commented on a number of other issues.

4. It was made clear by those responding that the telecommunications industry (the industry) remains committed to the fight against terrorism. However the 'voluntary' nature of the code appears to pose considerable difficulties which prevent the industry from delivering an adequate business case to its respective management boards in support of a voluntary regime.

5. On the question of the appropriateness and proportionality of the code, many of those responding indicated that they did not feel the threat to national security was a subject on which they had sufficient knowledge to enable them to judge the extent of the proposals. Of the replies received 34 commented on this issue and, of those, 25 believed that based on the information available the approach was not appropriate or proportionate.

6. The validity of data retention under the code, in relation to data protection legislation, provoked comment from 27 respondents. Of those, 22 believed that the regime would be inappropriate. Some comments highlighted difficulties that an individual company might face after volunteering, when making a decision as to the 'necessity' of the retention of the data. A combined response from a group of operators stated that 'since compliance

with the proposed Code of Practice would be voluntary, it falls to CSPs to determine that the measures are necessary, proportionate and justified for the purposes of national security.' It was stressed that this would leave the industry in a vulnerable position. The industry indicated that it was looking for a clear lawful basis for data retention.

7. On the question of whether the industry could comply with Appendix A of the code only 16 of those replying commented. Many of them identified the practical and technical difficulty involved in complying and the fact that the voluntary nature of the code could result in parts of the industry being 'voluntarily 'taxed'. Some indicated that they were unsure of the industry position as a whole, whilst others highlighted the difficulties within their own company infrastructure. The statement that business is 'being driven by other influences to hold data only when that was vitally necessary for business' gave an indication that compliance with the code may conflict with business plans.

8. Cost recovery was a relevant factor for most of those who passed comment. The methods currently deployed to access data retained for business purposes do not necessarily mirror the needs of the law enforcement agencies. It was commented that significant costs would be incurred by the industry to design and produce systems that could cope with the search and retrieval requirements of requests from the law enforcement agencies. Despite this the responses showed a clear split in opinion, with some positive attitudes to compliance capability being expressed.

9. The ability to judge whether the cost of compliance justified the end result provoked comments on the lack of a costed business case in the consultation paper. Of the responses 7 felt the end result would be justified whilst 16 expressed the opposite opinion. However concerns were expressed on both sides over the need to ensure that the impact of related costs were borne by the Government rather than the industry. ISPA UK indicated '…there are a number of direct and indirect costs that CSPs who comply with the Code will face. This comes at a time when the communications industry continues to face severe financial difficulties and instabilities.'

10. Two thirds of those who contributed to the consultation process expressed a view on the need for a retention regime. Of these, 22 were against the concept of retention, whilst 14 favoured such a regime. The Information Commissioner highlighted the policy of Data Protection Commissioners across the EU and stated that 'he would have preferred greater reliance to be placed on data preservation.' However, the law enforcement and intelligence agencies responses strongly emphasised the fact that data preservation is only a useful tool when used in conjunction with data retention.

11. Of the total responses 26 contained comment on the retention timescales proposed in the Appendix to the Code of Practice. Nineteen of these indicated that the periods identified were not reasonable. ISPA UK believed that 'compliance with the Code will result in a number of practical and technical difficulties for CSPs…. retaining data for extra time periods will lead to storage problems, particularly for the larger CSPs….. data processed for business purposes are not retained in a way that is usable by LEAs.'

12. Cost implications and issues surrounding the impact on the industry were a concern to 31 respondents. Twenty-six indicated that the retention proposals would have an adverse effect on the industry unless fully supported by Government. The APIG enquiry concluded that '…data retention will be immensely expensive and even with Government assistance on costs will consume engineering resources that the CSPs wish to devote to other, profitable projects.' Other responses indicated that 'substantial investment is required to meet the requirement …..unless it is clear at the outset that such investment can be fully recouped, it is difficult to justify significant capital expenditure for a discretionary project generating no commercial return.'

13. The question of the disparity between the retention and access regimes was mentioned in 25 responses. Twenty-four of those considered the matter as a problem that needed to be resolved. One respondent commented 'There is a legal view that while the retention may not in itself be unlawful, there is a significant risk that the collateral use of such retained data beyond investigations relating to national security would infringe an individual's right.'

14. Broadly speaking the comments delivered during the consultation process encompassed the issues of legal exposure including the Human Rights implications, competitive neutrality and cost recovery. The consensus was that a voluntary approach was unable to resolve these matters and that the voluntary nature of the Code would not deliver an 'across the board' solution and clearly, issues of national security demand such a resolution.

15. The industry indicated their view that it was necessary to ensure retention was on a firm lawful basis. The Information Commissioner indicated if there was a need for such retention, the Commissioner would prefer this to be on the basis of a statutory duty which would provide a greater degree of certainty than is possible with this voluntary arrangement.

16. However, respondents also considered that the introduction of a mandatory regime under the Anti-Terrorism, Crime and Security Act would still leave the issue of disparity unresolved and, in their view, additional legislation would be needed to resolve their concerns.

Conclusion

17. The consultation paper provoked a lively debate about data retention across a broad spectrum of interested parties and reconfirmed industry's commitment to helping the government achieve its aims in the fight against terrorism.

Home Office
September 2003

List of those responding:

All-Party Internet Group
The Local Government Staff Commission for Northern Ireland
Stephen Berry
The British Computer Society
Stephen Mason
British Phonographic Industry Ltd
Steven Mathieson
BT
Microsoft
Daniel Clift
Norfolk Constabulary
CBI
Northern Ireland Ambulance Service
CSP Operators Group
Northern Ireland Fire BrigadeStephen Coast
Northern Ireland Counter Fraud Unit Department for Trade & Industry
NIACT
Data Protection & Privacy Practice
O2 (UK) Ltd
Mark Dziecielewski
Orange UK
Energis
Diana Plummer
EURIM (The European Information Reuters Society Group)
Royal Mail
European Competitive
Scottish Advisory Committee on Telecommunications Association Telecommunications (SACOT)
Matt Freestone
Stand.org.uk
Freeserve
Chris Sundt
FIPR (The Foundation for Information Policy Research)
T-Mobile (UK)
Telenor Business Solutions Ltd
GreenNet
Liz Thompson
David Hansen Thus plc
IEE (The Institution of Electrical David Tomlinson Engineers)
UKERNA
The Information Commissioner Vital International Ltd
Vodafone Limited
Intellect (Information Technology Telecommunications & Electronics Association)Internet Service Providers Association UK (ISPA UK)

The Law Society
The Law Society of Scotland
Leeds University
Liberty