

**Information Commissioner's response to
"Protecting the Public in a Changing Communication Environment"**

A consultation by the Home Office

1.0 Introduction

1.1 The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998, the Freedom of Information Act 2000, the Environmental Information Regulations and the Privacy and Electronic Communications Regulations. He is independent from government and promotes access to official information and the protection of personal information. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The comments in this consultation response are primarily from the data protection perspective.

1.2 The proposal to ask Communications Services Providers (CSPs) to collect more communications data and then conduct further processing of those data raises a number of concerns from a data protection perspective. The second data protection principle states:

'Personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.'

It is vital that individuals are protected by strict and specific provisions being included on the face of primary legislation to limit the purposes for which additional communications data is collected and further processed. There should not be any room for this data being used by CSPs themselves for any other commercial or internal business purposes. Limitations on access and use should be framed precisely and appropriate sanctions should be in place for CSPs who misuse personal data or for their employees where appropriate.

1.3 The third data protection principle states:

'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'

Based on the evidence presented in the consultation, and further documentation available to us, the Information Commissioner believes that the case has yet to be made for the collection and processing of additional communications data for the population as a whole being relevant and not excessive. It is important to note that while the consultation presents this as maintaining a capability, this will in effect involve the collection and processing of a significant amount of additional information not previously available to CSPs and police and intelligence services. There are questions to be asked about the utility of the majority of the additional communications data that are to be collected and therefore their relevance to police or intelligence investigations.

1.4 The fourth data protection principle states:

‘Personal data shall be accurate and, where necessary, kept up to date.’

It is important to consider the diversity of communications data that are currently in use, from mobile phone communications to mobile and fixed line internet, Voice Over Internet Protocols, webmail services, gaming platforms and social networking sites. We are aware that some CSPs are concerned that it will be very difficult and prohibitively expensive to link accurately communications data collected with their own service users and even more difficult with their associates. This raises particular concern for us as a data protection regulator in relation to the individuals who may be mistakenly identified through use of this communications data.

- 1.5 Any proposed extension of the existing arrangements providing law enforcement bodies with access to records of personal communications is bound to provoke concerns about individual privacy and whether the measures are justified. We should remember that communication records – who? when? where? – can be highly intrusive even if no content is collected. One can tell much about an individual’s personal circumstances from the people they are talking to and the websites they visit. It is important that the proposals are tightly defined and minimise the level of intrusion and that appropriate safeguards are put in place.
- 1.6 This proposal represents a step change in the relationship between the citizen and the state. Prior to this, police and intelligence services would have access to information which was already collected and held by CSPs. For the first time this proposal is asking CSPs to collect and create information they would not have previously held, and to go further in conducting additional processing on that information. Evidence for this proposal must be available to demonstrate that such a step change is necessary and proportionate.
- 1.7 The Information Commissioner welcomes the fact that the consultation document rejects the proposal that all of the additional data collected be kept in a single database, held by the Government or a central agency. The Home Office recognise that a single database would be a step too far and appreciate that privacy concerns are engaged by the increasing collection and retention of communications traffic data.
- 1.8 The Commissioner is concerned about the distinction being made between traffic data and content data of any communication. All communications over the internet involve packets of data, with the traffic data at the beginning and end of the data packet. But if an individual is using a third party communications provider, hosted on his communications service provider (CSP), then the traffic data in the packet will only show the recipient as being the third party provider. Details of the final recipient of the communication will be held in the content of the packet. While the consultation makes it clear that CSPs will be required to conduct some further processing of third party communications data to match it with their own business data, it does not make it clear that this will necessitate some processing of data from the contents of the packet.

- 1.9 In terms of the substance of the consultation, references to safeguards might imply that the Information Commissioner has a greater role in the oversight and regulation of the use of interception of communications than is actually the case. The Information Commissioner is concerned that there may be gaps in the current regulatory regime that not only have the potential to affect the rights of individuals and their avenues of recourse, but also the clarity of roles and responsibility of CSPs.
- 1.0 While the interception of communications falls outside of the Information Commissioner's regulatory remit, the Information Commissioner's Office (ICO) receives many complaints from individuals who do not understand what is a very complex and sometimes opaque, regulatory regime. Indeed, even the Government have struggled in fully understanding where the ICO regulatory competence begins and ends when it comes to communications data¹.
- 1.11 The ICO has been criticised by campaign groups who believe that the ICO is trying to avoid taking action on alleged interception of communications by commercial organisations. In light of this, the evidence in this submission will detail the Information Commissioner's view on some of the current gaps in the regulation of interception of communications. The outgoing Information Commissioner has already made his concerns about potential gaps in the regulation of interception of communications a matter of public record in his final submission to the House of Lords Constitution Committee during their inquiry 'Surveillance: Citizens and the State'².
- 1.12 The consultation poses a number of specific questions. The next four sections of this document will detail the ICO's response to these questions.
- 2.0 On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public?**
- 2.1 The Information Commissioner accepts that communications data can be an important tool in tackling serious crime, preventing terrorism and protecting the public. However there are several reservations which mean the answer to this question cannot be an unqualified 'yes'. Accepting the value of communications data does not necessarily mean support for the general use of interception technology covering the population as a whole.
- 2.2 One reservation is that just because certain communications data have proved useful in certain cases where a specific individual, or group of individuals, has been identified, it does not necessarily follow that the collection of the communications data of the entire population will be useful in any but a tiny minority of cases. The value of information gained through the interception of communications of specific, identified individuals does not in itself justify the

¹ See the Government's petition response to the ISP Phorm petition at <http://www.number10.gov.uk/Page19318>

² Available on the ICO website www.ico.gov.uk

general collection, processing and retention of communications information covering the population as a whole. The case has not yet been fully made out for routine collection and retention of further communications data covering the entire population.

- 2.3 Questions need to be answered, particularly in light of the implementation of the European Data Retention Directive³ into United Kingdom law⁴, as to whether further routine collection of communications data is actually necessary or whether it is more expedient only to collect further communications data if and when an individual becomes a suspect and further communications data is needed for the investigation. Is the best use currently being made of what is already available for the police and intelligence services? If the intention of Government is to ensure that this information is available when needed in specific cases, and therefore that communications data relating to individuals who are not suspects will not be routinely profiled, then it is more difficult to justify the mass retention of additional communications data covering the entire population.
- 2.4 While the value of accessing communications data as part of an ongoing investigation is not in doubt, it is harder to make a case for the collection of even more communications data on a population-wide scale “just in case”. However, if an individual becomes a suspect in an investigation of a serious crime or terrorist act, then it is perfectly reasonable, indeed desirable, that the authorities then have the power to compel the collection of further communications data in relation to that individual, and in many cases their associates. This would enable a picture of a suspect’s movements online to be drawn up and would inform any decision for monitoring and surveillance of the content of communications. Another option might be to target the collection of communications data on particular media.
- 2.5 A second reservation is that the definitions in the conditions under which communications data can be accessed by a relevant public authority are often too widely drawn and can lead to misuses of the rights of access of public authorities to such information. There has been much public debate about the inappropriate use of powers under the Regulation of Investigatory Powers Act 2000, and this must not be allowed to happen under any new legislation brought before Parliament. If the Government is to justify its proposals on the grounds of preventing serious crime, terror and substantial threats to public health, then the legislation must not be so broadly framed as to allow too broad access and use by having to imprecise conditions being applied by too broad a cross section of public authorities. If this happens, such proposals are unlikely to command public trust and confidence.
- 2.6 Definitions of what constitutes “serious crime”, “terrorism” and “protecting the public” and strict limits on the conditions for accessing communications data should be laid down in primary legislation. Significant amendments to the list of bodies that can access the data must be debated in Parliament, not merely

³ DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

⁴ Implemented as the Data Retention (EC) Regulations 2009

subject to order making powers. It is important that the foundations of the safeguards that the Government talks about later in the consultation are laid firmly in the primary legislation, and that those safeguards are strong enough to stand up to any potential misuses, including well-meaning but misguided function creep. Audit trails of who has accessed what communications data should be mandatory and there should be effective oversight and well-publicised recourse if information is accessed inappropriately.

- 2.7 The ICO has direct experience of dealing with some of the complaints that arise under the current mosaic of regimes that govern the various forms of surveillance in the UK. In particular cases come to the ICO about access to various forms of communications data which have been collected through interception of communications.
- 2.8 The first data protection principle states that processing of personal information must be fair and lawful. Any processing of personal information which has been obtained in contravention of the provisions of section 1(1) of RIPA would also be in breach of the first principle. Understandably organisations approach the ICO for advice. However, it is inappropriate and arguably beyond his powers for the Information Commissioner to advise on the lawfulness of interceptions of communications under RIPA. He does not have particular expertise in this area. An organisation could follow the advice of the Information Commissioner but still be liable for prosecution if the prosecuting authority for RIPA takes a different view.
- 2.9 Section 57 of RIPA creates the role of Interception of Communications Commissioner, but his role is limited to overseeing the persons who issue warrants, and the procedures of those who are acting under warrant or who are assisting those acting under warrant. RIPA places no duty on the Interception of Communications Commissioner to provide advice to those who are not covered by RIPA, mostly private sector actors, who want to ensure they are acting in a manner which is in compliance with RIPA, nor is he resourced to provide such advice.
- 2.10 The Interception of Communications Commissioner has no remit to investigate complaints about those bodies outside RIPA who have contravened the requirements for “lawful interception” of communications. This also applies to the Investigatory Powers Tribunal. Effectively, what this means is that where the private sector, either through their own provision of services, or through being placed under a legal obligation, are intercepting communications of services users, there are gaps in the regulatory regime. The only recourse for a private sector breach is prosecution for a criminal offence. This is different from the position that applies to the public sector. Arguably there is a need for an appropriately empowered regulator, who can provide advice and guidance and ultimately impose civil sanctions against private sector players.
- 2.11 In contrast, when the ICO is approached for advice as to the application and applicability of data protection law, the ICO is empowered to provide such advice under section 51 of the Data Protection Act 1998. Indeed, the ICO is under a specific obligation to promote the following of good practice which includes but is not confined to compliance with the requirements of data protection law. The problem is that whilst the DPA and RIPA together form part

of the framework of regulation that limits excessive surveillance and provides safeguards for individuals it is only in relation to the DPA that there is an organisation charged with promoting compliance with the legislation and with providing authoritative advice to those who need it.

- 2.12 CSPs will need regulatory clarity on what is and what is not permissible when devising the means of collecting and processing communications data. Regulatory uncertainty will present commercial and privacy risks that will be difficult for them to manage. This is particularly important because the current regime presents no effective means for CSPs to get advice or direction until after they have committed a possible criminal offence. This is equally unsatisfactory for individuals who may feel that an unlawful interception of a communication has taken place but who have no obvious means of redress if they cannot convince the police that a prosecution is in the public interest.
- 2.13 A final issue of safeguarding the additional data needs to be considered. While the Data Protection Act 1998 provides general protection for personal data and sanctions for those who misuse it, the Information Commissioner believes that additional limitations need to be placed on CSPs exploiting the additional communications data they will be obliged to process for commercial purposes. In a world where CSPs are constantly looking at how the information they hold on service users can be used for better targeting of other commercial services they provide, it is essential that strict and specific limitations are placed on the use of this data. There must also be appropriate sanctions for CSPs who use the additional communications data for commercial means, or for individuals employed CSPs or third party contractors who misuse or disclose the information they collect and process. There must be strict limitations on who can access this data within CSPs and audit trails on access that can be monitored effectively.
- 3.0 Is it right for the Government to maintain this capability by responding to the new communications environment?**
- 3.1 If one accepts that communications data is vital in some circumstances to the prevention and detection of crime, the apprehension or prosecution of offenders, prevention of terrorist acts and/or the protection of the public, then it is logical that action should be taken to identify and address significant gaps in the types of useful communication data which are potentially available to the police and other appropriate public authorities. This is not though a justification for universal collection of communications data or for unfettered access to those data by named public authorities.
- 3.2 Again, the answer to this question is not a straight “yes or no” and it is highly dependent on which option the Government chooses, the safeguards it puts in place and how the option is implemented. What is important is that the arrangements for collection and access to communications data are proportionate and reasonable. In some cases proportionate and reasonable arrangements will maintain or could even enhance the existing capability. However, with some news communications technologies simply seeking to maintain an existing capability may be neither proportionate nor reasonable.

4.0 Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?

- 4.1 The ICO cannot provide a direct answer to this question because of the lack of detail about the options presented in the consultation, and the nature of the safeguards which are to be put in place. At this stage and before any final details are clarified, we consider the first part of this question will not necessarily inform the debate – and, consequently, we must reserve our position.
- 4.2 Several solutions to maintaining capability do not appear to have been considered by Government, or at the very least not detailed in this consultation. At present, the consultation only looks at three options:
- A single store, which is rejected on the grounds that the implications for personal privacy might be too great.
 - Doing nothing.
 - The single, proposed 'middle way' of asking CSPs to store further data on every subscriber's use of third party communications services being hosted on their networks.
- 4.3 The consultation states that if the single store solution is rejected, then the remaining two options are the only other options available. The ICO would suggest that there is at least one further viable option available to the Government which has not been detailed in the consultation and which has been discussed briefly above.
- 4.4 Has the Government considered bringing forward legislation that would allow specified public authorities to request that this further communications data be collected only in relation to specified individuals, and possibly their associates, who have come to the attention of those authorities by other means? Or have they considered only collecting communications data from the media where there is greatest risk? Another option could be that specific phone numbers or circumstances could be targeted. These and other alternatives would be less intrusive than obliging all CSPs to collect this further communications data on all subscribers and more justifiable as it would be targeted and collect a narrower range of information about fewer individuals.
- 4.5 Such a targeted use of communications data could also simplify the day to day operational judgments of proportionality and necessity were applied to access such data, as these factors would have already have been assessed when the decision to start collecting such data was made. If the Government have considered other alternatives, these have not been detailed in the consultation document. If the alternatives are not considered feasible, there is no information in the public domain as to why this might be.
- 4.6 We would also point to the approach taken by the financial industry over money laundering. The 'know your customer' approach leads to more selective checks being undertaken on customers who pose a greater risk. As such a trusted customer is not subject to the same checks as a non-trusted customer. As a result the collection of data on money transfers is more targeted, less intrusive and much less resource intensive. The current proposal to have CSPs collect further communications data about every customer seems less selective, is

arguably less proportionate and appears to be responding to the new communications environment by arguing for doing more of the same, rather than looking for more flexible, innovative and privacy friendly solutions.

- 4.7 A final issue to consider is whether the UK has given the current arrangements enough time to work and has not learned from the experience of the recently introduced Data Retention Directive⁵. This has only been recently implemented into UK law and it is important to see how useful this legislation is to police and intelligence services before arguing for yet more communications data to be collected.

5.0 Conclusions

- 5.1 The ICO recognises the value that communications data has for the prevention and detection of crime and the prosecution of offenders. However, this in itself is not justification enough for mandating the collection of all possible communications data on all subscribers by all CSPs.
- 5.2 The ICO is concerned that the current safeguards are not adequate to deal with the further collection and processing of communications data by CSPs. Indeed the gaps in regulatory oversight carry an inbuilt risk of non-compliance with current law surrounding interception of communications. Not only does this carry privacy risks, it also presents significant commercial risks for CSPs in that the only oversight is when a criminal offence has been committed.
- 5.3 The consultation does not appear to have fully investigated other options that may exist between the two extremes of a single, centralised Government database of all communications data and doing nothing. The ICO response presents several other options that need to be properly considered and open to public debate and comment. Full consideration of all available solutions is essential to ensuring that the final decision as to which option is selected fully considers the proportionality and necessity of that solution against other possible solutions.

⁵ DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
15 July 2009