LIBERTY80

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's response to the Home Office consultation on the Acquisition and Disclosure of Communications Data and the Retention of Communications Data Codes of Practice

January 2015

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

Isabella Sankey
Director of Policy
Direct Line 020 7378 5254
Email: bellas@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sara Ogilvie
Policy Officer
Direct Line 020 7378 3654
Email: sarao@liberty-human-rights.org.uk

Introduction

1. This is Liberty's response to the Home Office consultation on the *Acquisition and Disclosure of Communications Data* and the *Retention of Communications Data Codes of Practice* (the *Acquisitions Code* and the *Retention Code*). This response also includes comments on the updates to the Retention Code that will be implemented in the event that Parliament passes the Counter-terrorism and Security Bill. The consultation paper states that proposals to update the Acquisition Code and the creation of the Data Retention Code are a result of the passage of the Data Retention and Investigatory Powers Act (DRIPA) in July 2014. That piece of legislation was introduced following the decision of the Court of Justice of the European Union (CJEU) in the *Digital Rights Ireland* case that the European Directive governing the retention of communications data was unlawful. As well as striking down the Data Retention Directive, the judgment also set out the parameters of a lawful data retention regime. Liberty considers that the Data Retention and Investigatory Powers Act does not comply with the requirements set out in Digital Rights Ireland and is incompatible with the Human Rights Act 1998. We are representing David Davis MP and Tom Watson MP as they challenge the legislation.

2. The principles set out in Digital Rights Ireland must be reflected in primary legislation in order to offer the strongest guarantee that the rights to privacy and freedom of expression will be protected. It is deeply concerning that the Government did not legislate in this manner. While we do not consider that provisions in Codes of Practice could compensate for the deficiencies of primary legislation, the Codes in any case do not respond to the requirements set out in by the CJEU. In particular, the consultation cover paper suggests that the Digital Rights Ireland requirements as to independent authorisation, protection of professionally protected correspondence, and international cooperation are all addressed adequately by the Codes. In this response we set out why this is not the case.

3. When the Government was pushing DRIPA through Parliament it claimed that the legislation did not in any way extend the surveillance powers of the state and did not seek to replicate the Draft Communications Data Bill. We also set out why this is incorrect and demonstrate that the changes introduced by DRIPA, when read in correspondence with the new provisions in the Counter-terrorism and Security Bill, grant to the state access to hugely increased amounts of communications data.

Digital Rights Ireland

4. The EU Data Retention Directive 2006/24/EC imposed an obligation on Member States to adopt measures to ensure that communications data generated or processed by providers of public communications services or networks within their jurisdiction be retained for 6-24 months and stored in such a way that it could be transmitted upon request to the 'competent authorities' without delay. Implementation of the Directive in UK law was achieved through the Regulations in force on 6th April 2009. The Regulations created the power for the Home Secretary to require communication service providers to retain communications data that they already held for business purposes for a prescribed period of 12 months.

5. The *Digital Rights Ireland* case ruled on the validity of the Directive following a referral by the High Court of Ireland and Verfassungsgerichtshof (Constitutional Court, Austria). The CJEU declared the Directive to be invalid as its provisions were incompatible with the rights guaranteed under Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union.[1] It concluded that the Directive entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary. The Court found that the EU legislature had "*exceeded the limits imposed by compliance with the principle of proportionality.*"[2]

6. The CJEU identified several characteristics of the Data Retention Directive that rendered the regime disproportionate. The effect of this was to define the limits of permissible data retention pursuant to human rights law and EU law. The court set out the following ten principles for a data retention regime –

- restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);
- provide exceptions for persons whose communications are subject to an

[1] Article 7 of the Charter of Fundamental Rights & Freedoms protects Respect for Private and Family Life and Article 8 provides for Protection of Personal Data. Article 52(1) requires that any limitations on the rights recognised under the Charter must be proportionate and necessary to meet the objectives of general interest recognised by the Union. The Charter is available at - http://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[2] Digital Rights Ireland case, para 69.

obligation of professional secrecy (paragraph 58);

- distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);
- ensure retention periods are limited to that which is 'strictly necessary' (paragraph 64);
- empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary (paragraph 62);
- restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);
- limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);
- ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access (paragraph 66);
- ensure destruction of the data when it is no longer required (paragraph 67); and
- ensure the data is kept within the EU (paragraph 68).

Data Retention and Investigatory Powers Act and the Regulation of Investigatory Powers Act

7. Provisions governing data retention are set out in the Data Retention and Investigatory Powers Act (DRIPA), which was introduced via emergency legislation in July 2014 as a response to the judgment in Digital Rights Ireland. The regime for acquiring data continues to be set out in the Regulation of Investigatory Powers Act 2000 (RIPA). Instead of reflecting the principles set out in Digital Right Ireland, the DRIPA regime allows for mandatory blanket communications data retention covering the entire population for up to 12 months without any nexus to the prevention or detection of serious crime, nor the other privacy safeguards laid out in the judgment. Under section 1 the Home Secretary can mandate, by order, the retention of 'relevant communications data' including 'all data' for a period of up to 12 months for any of the broad purposes set out in section 22(2) paragraphs (a) to (h) of RIPA which include for example the assessment of taxes and the prevention of disorder.

8. DRIPA also failed to narrow the loose and lax communications data access regime for public authorities' provided by Chapter 2 of RIPA and under the section 25(1) Regulation of Investigatory Powers (Communications Data) Order 2010. The law currently authorises the acquisition of communications data by hundreds of public authorities and most public bodies are able to authorise internally their access to communications data for the same broad range of purposes under which communications data is retained. Barring local authority access, there is no requirement for independent prior judicial authorisation when communications data is sought by public bodies.

9. DRIPA provides for wide scale privacy infringement. Since the 2009 Regulations have been in force, communications data has been accessed on a massive scale in the UK with roughly half a million requests from public bodies per year. The rules governing targeted surveillance make it impossible to know with any certainty the scale of disproportionate use and abuse of communications data by public authorities but the sheer volume of requests and inadvertent examples of bad practice make clear that it is a serious problem. In 2013, 869 communications data errors were reported to the Interception of Communications Commissioner and a further 101 identified during his random inspections. Several communications data errors had "very serious consequences" including warrants being "executed at the homes of innocent account holders and this is extremely regrettable."[3]

Independent Authorisation

10. The requirement that communications data can only be accessed following judicial authorisation or authorisation by an independent body is contained in paragraph 62 of Digital Rights Ireland, which criticised the fact that under the Directive, *"the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary."*

11. This requirement for prior external authorisation is not provided for in either DRIPA or RIPA. In Part 1, Chapter 2, Section 22(3) RIPA, authorisation to access communications data may instead be granted by a designated person who works

[3] Interception of Communications Commissioner, Annual Report 2013, page 36 at paragraph 4.51.

within the same public authority as the person requesting the data. Following the *Protection of Freedoms Act 2011*, local authorities must undergo a process of prior judicial authorisation. It is unclear why in the light of Digital Rights Ireland the Government did not extend a prior judicial authorisation regime to all access arrangements. Paragraph 3.7 of the updated Acquisition and Disclosure Code sets out that *"If the designated person believes the acquisition of communications data is necessary and proportionate in the specific circumstances, an authorisation is granted or a notice is given."* Paragraph 3.11 states that *"Designated persons must be independent from operations and investigations when granting authorisations or giving notices related to those operations."* From paragraphs 3.12 onwards, it is set out that where it is necessary to act urgently, the designated person need not be independent from the investigation or operation concerned.

12. Despite the efforts of paragraph 3.11 to state that designated person must be "independent" of the investigation concerned, when authorisation is granted internally the requirement of independence can never truly be met. Independence requires decision making to be made by separate institutions with constitutionally distinct responsibilities, not individuals, as is made clear by the statement in Digital Rights Ireland that authorisation must be made by *"a court or independent administrative body".* We do not seek to impugn the integrity of public officials or senior employees of our law enforcement agencies, but rather point out the reality that their primary concern will relate to the operational capacity of their agency. This is a matter of organisational culture and is perfectly understandable, but it is also a reality which militates in favour of independent third party authorisation. Decisions concerning necessity and proportionality can only be properly made by someone without any conflict, or perceived conflict, of interest. It is also significant that the Code also goes on to provide that even this very weak requirement of internal independence need not be met in every case. It is clear that the system of authorisation set out in the Acquisition Code in no way matches the high standard of independence identified in Digital Rights Ireland.

Professionally privileged communications

13. At paragraph 58 of Digital Rights Ireland the mass nature of data retention was criticised, with particular emphasis placed on the lack of protection in the EU Data Retention Directive for those whose communications are subject to obligations of professional secrecy. The consultation cover paper noted the recent revelations in the UK that the police have been using RIPA to access communications data of

journalists in order to identify journalistic sources and asked for comments on whether the relevant provisions in the code protect freedom of expression.

14. However the Acquisition Code's section on communications data involving certain professionals – such as journalists, lawyers and doctors – offers little indication that this issue is being taken seriously by Government. Paragraph 3.72 of the Code states that *"communications data is not subject to any form of professional privilege – the fact that a communication data took place does not disclose what was discussed, considered or advised."* Liberty strongly challenges this outdated notion of communications data as largely unrevealing and undeserving of the protections offered to material the government classes as privileged. Consider the range of situations in which just the fact of a single communication and the identity of the parties speaks volumes: the phone call from a senior civil servant to a Times reporter immediately before a major whistle-blower scandal fills the front pages, the email to a civil liberties watchdog from a police officer during the course of an inquest into a death in police custody. In these kinds of circumstances, communications data can be just as revealing as the content of a communication. We would strongly encourage the government to rethink its definition of "privileged" material.

15. Paragraph 3.74 states that when an application is made for the communications data of a medical doctor, lawyer, journalist, Member of Parliament, or minister of religion, the applicant must give *"special consideration"* to necessity and proportionality and the designated person must take *"particular care"* when considering applications. These requirements are surely the minimum standards that we should expect any applicant or designated person to take in each and every case. It is deeply concerning that these precautions would only be taken in special circumstances rather than be part of the normal processes. In addition, these weak provisions in the Acquisitions Code do nothing to nothing to address the concern of the CJEU that professionally privileged communications require special protection in terms of the *retention* regime.

16. The consultation paper suggests that the Government is giving consideration to "flagging" all applications for communications data of those who work in professions that handle confidential information with the Interception of Communications Commissioner at his next inspection. We do not consider that one-off, after-the-fact review of applications offers anywhere near the level of scrutiny required by Digital Rights Ireland. Requiring in primary legislation prior judicial

authorisation for all attempts to access communications data is the bare minimum safeguard that must be introduced.

Arrangements for disclosure to overseas authorities

17. In Digital Rights Ireland, the court highlighted the lack of legislative safeguards to secure effective protection against the risk of abuse and unlawful access to data, and in particular noted that there was nothing to require data to be kept within the EU and subject to the rules governing data protection. Paragraph 7.18 of the Acquisition Code asserts that *"Where a UK public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring data to that authority, it must consider whether data will be adequately protected outside the UK."* Paragraph 7.22 then adds *"There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a decision that can only be taken by the public authority holding the data on a case by case basis."* In Digital Rights Ireland, at paragraph 66 the CJEU was clear that the lack of rules *"to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality"* rendered the EU retention regime unlawful. The relevance of this point to transfers of data outside the EU was then made explicit at paragraph 68. The complete failure to set out the precise safeguards that will apply to transfers of information and the suggestion that sometimes there will be no safeguards contradicts the requirement for "explicit" and "strict" safeguards.

18. The most appropriate way for Government to seek to access information held overseas or to share information with overseas authorities the use of Mutual Legal Assistance Agreements (MLATs) with other States. MLATs operate under the Crime (International Co-Operation) Act 2003 and allow for the sharing of information between States for the purposes of detecting and prosecuting crime. They provide a transparent framework, avoiding the legal complexities and human rights risks of States seeking to act unilaterally, leaving service providers as the only barrier against privacy violations. Not only do they offer the best way of ensuring that safeguards are applied internationally, but they have the capacity to be an extremely effective method for the transfer of information. The Government has claimed that the MLAT system is too slow and bureaucratic to be an effective mechanism. However MLATs

are wholly a product of Government – the terms are decided by Government, they are implemented by Government and they are funded by Government. It is difficult to see why, with commitment and leadership, inefficiencies cannot be reduced and MLATs turned into a useful, human rights compliant model for information sharing between states. The vague assertions in the Acquisition Code that it is necessary to act on a "case by case" basis rather than take the opportunity to reaffirm a clear commitment to the MLAT system and direct the use of it in these cases is puzzling.

Data retention notices

19. Paragraph 1.9 of the Data Retention Code confirms that *"The Home Office does not publish or release identities of CSPs subject to a data retention notice as to do so may identify operational capabilities or harm the commercial interests of CSPs under a notice."*

20. It is extremely concerning that the privacy of potentially the entire UK population can be violated via secret notices. It is exceptionally difficult to bring a legal challenge against a notice that is secret. Given that this provision adds to existing layers of secrecy in the data communications regime – for example, individuals whose communications are accessed are not informed of the fact – the result is likely to be that the Secretary of State is effectively absolved from accountability for the lawfulness of her decision-making. It is telling that the reasons given for keeping notices secret prioritise the commercial interests of the CSPs while making absolutely no reference to human rights obligations of the state.

Counter-terrorism and Security Bill

21. Section 17 of the Counter-terrorism and Security Bill (CTSB), which is currently passing through Parliament under a fast-track process, makes a number of changes to DRIPA. Sections 4 and 5 of DRIPA already represented an extension of the state's powers as compared to the previous Data Retention Regulations. The Retention Code addendum, which outlines changes to the Code should the CTSB pass, makes clear the way in which these sets of changes will extend the reach of the communications data retention regime.

22. Under Section 1 of DRIPA, companies can be required to retain data that is already generated or processed in the UK as part of their normal business

operations. Companies are not currently required to retain data that they would not normally log for their own business purposes. The CTSB will alter this obligation by mandating certain types of communications data that companies must generate and store, regardless of whether this is data which is usually retained for business purposes. The Government states that this provision is necessary because internet companies do not currently have the information required to show which IP address was being used by which user at a given point in time. In principled terms, this marks a significant shift in the relationship between the state, companies and services users, co-opting companies into the surveillance process in a novel way and it would grant the state some of the powers (to require companies to generate new information) it sought in the DCDB. For the Government to rush through this type of change in fast-track legislation, which also piggy-backs on emergency legislation, shows a contemptible disregard for parliamentary process as well as the civil liberties of the millions on innocent individuals affected by the proposals.

23. In practical terms, the provision will lead to the creation of huge amounts of additional data about internet usage. Section 17(3) sets out that the Secretary of State can mandate the retention of *"communications data which (a) relates to an internet access service or an internet communications services and (b) may be used to identify, or assist in identifying, which internet protocol address, or other identifier, belongs to the sender or recipient of a communication (whether or not a person)"*. The only exemptions to this mandatory retention are *"data which (i) may be used to identify an internet communications service to which a communication is transmitted through an internet access service for the purpose of obtaining access to or running a computer file or program and (ii) is generated or processed by a public telecommunications operator in the process of supplying the internet access service to the sender of the communication".*

24. Paragraph 1.7 of the addendum to the Retention Code states that these exemptions mean that companies subject to a notice will not be required to retain information on which websites an individual has accessed. However, the extent of this protection is extremely unclear. The revised Acquisition Code explains at paragraph 2.24 that "webpages" count as communications data, whereas "websites" do not. It is also the case that some IP addresses only attach to certain webpages, so the simple process of IP resolution will give away the type of information that the government seems to suggest will be hidden. Further, even if the Government's

purported explanation holds true and details of websites are not available, the knowledge that an individual has logged onto the internet at a particular time and place still produces a significant amount of information about that individual which could be hugely revealing.

25. At any given point, an IP address can potentially be linked to thousands of devices such as a phone or computer. This means that the process of matching IP addresses with users can be extremely complex and has the potential to involve large amounts of information about all of these individuals, including location, all of which would be retained under the Bill. Under Section 17(3)(b), the Bill also goes further than the government's stated intention. The information required to be retained is defined very loosely, even extending to information linking an individual not to an IP address but to any "other identifier", such as an email address or social media account handle. This provides the opportunity to link different online accounts and internet usage with one device or individual.

26. Under section 22 RIPA, a designated person within a public authority can authorise another person within that public authority to access communications data held by a company, or can issue a notice requiring the company to disclose communications data. Section 4(8) DRIPA purported to give this power extraterritorial effect, meaning that notices can now be issued against companies not based in the UK. Section 5 DRIPA also changed the meaning of "telecommunications service", and paragraph 2.5 of the Data Retention Code of Practice confirms that as a result, companies who provide "webmail" services can now be the subject of a data retention notice. This means that companies such as Google, Facebook and Twitter can all now be required to store and provide communications data. The combination of this power with the proposed mandatory requirements at section 17(3) CTSB means that the volume of communications data which must be generated and retained will increase substantially, and effectively gives the state access to what was termed "third party data" in the DCDB at source.

27. The information generated and stored under these new proposals will in part depend on the service provided by the company subject to a notice. Internet service providers (for example, BT Internet or Vodafone) will be able to record the type of device used, who was using that device, the fact that the individual logged into an

email server and sent a form of encrypted information. A company such as Google might be able to provide a much more detailed account of what happened, providing the exact email address that was used, the email address it was sent to etc. The Data Retention Code states explicitly at paragraph 2.6 that communications data to be retained includes information sent automatically from machine to machine. This may mean, for example, that when an individual's Twitter account updates automatically, the communications data generated by this – such as location – will be recorded each time this happens.

28. Paragraph 2.16 of the Acquisition Code of Practice confirms that the change at section 5 DRIPA also means that providers of wifi services – such as a hotel, a coffee shop, an airport – can all be required to share communications data. This means that locational information to be provided may be very specific, and at the same time may produce a detailed insight into the activities of the person using the device at any particular time. Similarly, the addendum to the Data Retention Code sets out an amendment to paragraph 3.25, that a data retention notice may include a requirement to retain transitory information in the core systems. This very fine-grained data about the route of a communication can provide very specific information about the route and transit of a communication.

29. The same section of the addendum adds that a notice may include *"a requirement to process the data to ensure that multiple items of data from a single or multiple CSP systems can be stored in a single clear record where appropriate to do so."* It is then suggested that the reason for doing so is *"to ensure the volume of data retained is limited to that which is truly necessary".* A requirement to process data represents a second additional privacy infringement. It will also allow for information to be stored in a database format paving the way for CSPs to be required to construct searchable databases as proposed under the DCDB and in previous legislative proposals. Given the way in which DRIPA and now the CTSB have both been used to introduce powers sought under the DCDB, the requirement to process data in this manner surely leaves open the door for a further piece of "emergency" legislation which will then grant the state powers previously sought, such as those to compile a searchable centralised database held by central government. We strongly suggest that this provision is removed.

30. When DRIPA was passing through Parliament in July 2014, Government Ministers repeatedly asserted that the legislation did not create any powers beyond

that which had previously been available under RIPA and the Data Retention Regulations, and was not an attempt to introduce provisions in the Draft Communications Data Bill via the backdoor. However, given that it will now be possible for government to: require the generation and retention of information not already required by service providers; require webmail and wifi companies to provide such information; require the mass processing of data on innocent people, it is no longer possible for this claim to be maintained.

Sara Ogilvie