PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT

First Delegated Legislation Committee

DRAFT DATA RETENTION AND ACQUISTION REGULATIONS 2018

Monday 15 October 2018

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Friday 19 October 2018

The Committee consisted of the following Members:

Chair: Sir Graham Brady

† Boles, Nick *(Grantham and Stamford)* (Con)
† Dakin, Nic *(Scunthorpe)* (Lab)
† Eagle, Ms Angela *(Wallasey)* (Lab)
† Goodwill, Mr Robert *(Scarborough and Whitby)* (Con)
† Hair, Kirstene *(Angus)* (Con)
† Hart, Simon *(Carmarthen West and South Pembrokeshire)* (Con)
† Maclean, Rachel *(Redditch)* (Con)
† Mann, Scott *(North Cornwall)* (Con)
† Maynard, Paul *(Lord Commissioner of Her Majesty's Treasury)*
† Morris, James *(Halesowen and Rowley Regis)* (Con)
† Newlands, Gavin *(Paisley and Renfrewshire North)* (SNP)
† Smith, Eleanor *(Wolverhampton South West)* (Lab)
† Thomas-Symonds, Nick *(Torfaen)* (Lab)
Twigg, Derek *(Halton)* (Lab)
† Wallace, Mr Ben *(Minister for Security and Economic Crime)*
† Williams, Dr Paul *(Stockton South)* (Lab)
† Yasin, Mohammad *(Bedford)* (Lab)

Yohanna Sallberg, Medha Bhasin, *Committee Clerks*

† attended the Committee

First Delegated Legislation Committee

Monday 15 October 2018

[Sir Graham Brady *in the Chair*]

Draft Data Retention and Acquisition Regulations 2018

4.30 pm

The Minister for Security and Economic Crime (Mr Ben Wallace): I beg to move,

That the Committee has considered the draft Data Retention and Acquisition Regulations 2018.

I am delighted to serve under your chairmanship, Sir Graham. The retention of and access to communications data is crucial in enabling investigators to obtain intelligence and evidence that can prevent terrorist attacks, disrupt the activities of serious and organised crime groups, and establish culpability so that offenders can be brought to justice. It is used to investigate crime, keep children safe, locate missing persons, support or disprove alibis and link a suspect to a crime scene.

The regulations introduce additional safeguards to ensure that the UK's regime complies with EU law. They also bring into force the code of practice of parts 3 and 4 of the Investigatory Powers Act 2016—IPA—the regime for communications data acquisition and retention. Between November 2017 and January 2018, we consulted publicly on the changes to the legislation and code of practice.

The regulations provide for the independent authorisation of communications data requests. The Investigatory Powers Commissioner, a senior judge, is given that power and will delegate the responsibility to a newly appointed body of staff, which will be known as the Office for Communications Data Authorisations.

OCDA will report directly to the Investigatory Powers Commissioner and will be responsible for considering the vast majority of requests made by public authorities to access communications data. The new body is expected to begin operating in April 2019 with independent authorisation being rolled out across public authorities during 2019. The internal authorisation of requests will continue to be permitted in urgent cases—for example, where there is a threat to life or where requests are made for national security matters, which are outside the scope of the European law.

The regulations restrict the crime purpose for which events data such as call histories and location information can be retained and acquired to serious crime. We have carefully considered how serious crime should be defined in the context of communications data—a decision that the European Court has rightly left to member states. We have worked with the operational community to focus on where communications data can be a valuable tool. Indeed, in some cases, it is the only investigative tool.

We have mirrored the definition that already exists in the IPA for the more intrusive interception and bulk powers, but we have adjusted the custodial threshold to one year, rather than three, to reflect the less intrusive nature of comms data. That will ensure that the power is not used in the investigation of low-level offences.

The definition also makes specific provision for offences that, as an integral part, involve the sending of a communication or a breach of a person's privacy, which will ensure that communications data can be used to investigate all harassment and stalking offences. Similarly, the definition extends to offences committed by corporate bodies, such as corporate manslaughter, where custodial sentences are not available. In addition, in every case, even where the serious crime threshold is met, an application for communications data can be authorised only where it is necessary and proportionate to what is sought to be achieved.

To ensure that the serious crime restriction can be brought into force on 1 November, the regulations amend the Regulation of Investigatory Powers Act 2000—RIPA. Until part 3 of the IPA is brought into force early next year, RIPA remains the legal framework for accessing communications data.

The new code of practice provides comprehensive guidance on the data retention and acquisition regime and describes roles and responsibilities, considerations that must be given and detailed processes that must be followed. The code takes account of the changes made in the regulations, in particular the role of the Investigatory Powers Commissioner and OCDA. It also provides further guidance on factors to take into account when considering the seriousness of offences in deciding whether communications data should be acquired.

The changes support the important right to privacy and the right of citizens to be protected from crimes and terrorism. They ensure that public authorities can continue to access retained communications data in a way that is consistent with EU law and our responsibilities to protect the public. The additional safeguards, the clear requirements set out in the code of practice and the independent oversight provided by the Investigatory Powers Commissioner establish clear limits around the use of the powers and provide reassurance for the public that communications data is being used only where it is necessary and proportionate. I commend the regulations to the Committee.

4.34 pm

Nick Thomas-Symonds (Torfaen) (Lab): It is a pleasure to serve under your chairmanship, Sir Graham; I thank the Minister for the information he has shared with the Opposition regarding this statutory instrument.

Following the ruling of the European Court that the Investigatory Powers Act 2016 was incompatible with European law, the Opposition welcome this instrument, which brings the legislation into line with that European law, together with the code of practice. We have accepted the ability of particular public authorities, including law enforcement and intelligence agencies, to have access to communications data, and we recognise that that can often be vital to ensuring public safety and national security. The proposed changes to the legislation and the code of practice would refine these data retention and acquisition regulations in two major ways: first, as the Minister has set out, by introducing an independent administrator who can authorise the use of these powers, and secondly, by,

"restricting the crime purpose for acquiring retained communications data to serious crime",

making the use of this power proportionate to the crime being investigated. We in the Opposition support strong powers and strong safeguards, and we welcome the refinement of this legislation.

While the Opposition are not opposed to these changes, I seek clarification from the Minister on one point. The divisional court has required that the Government make legislative changes to bring the Data Retention and Acquisition Regulations in line with European law by 1 November 2018. While I understand that the proposed serious crime threshold will take effect in November 2018, the Government have stated in their explanatory memorandum that,

"the associated requirements for independent authorisation",

will come into force from April 2019, six months after the deadline set by the court. The information provided by the Government cites complexity of implementation as the reason for that six-month delay, but I wonder whether the Minister can offer further clarification on the reasons.

As I have stated, the Opposition do not plan to oppose these changes, although I note that my former colleague, now the Mayor of Greater Manchester, Andy Burnham, warned the Government in June 2016, when the Investigatory Powers Bill was being debated, that the threshold had to be a precise one. He said that,

"we must…legislate to put in place a very precise threshold, so that the circumstances in which those data can be accessed are explicitly clear…we need a very clear definition of what level of crime permits the authorities to access those records."—[*Official Report*, 7 June 2016; Vol. 611, c. 1121.]

I am pleased that the Government have made the reasonable adjustments required to this legislation, so that that balance can now be appropriately struck.

4.37 pm

Gavin Newlands (Paisley and Renfrewshire North) (SNP): It is a pleasure to serve under your chairmanship, Sir Graham.

My colleague, my hon. and learned Friend the Member for Edinburgh South West (Joanna Cherry), opposed many of the measures in the Investigatory Powers Act during the Bill Committee and questioned whether many of the proposals were lawful. Now we know the answer, as it relates to what is in the 2016 judgment. Despite having opposed many of the measures in the 2016 Act, we have always said that we could support such measures if the Government proved the proportionality and necessity of the proposals. That has not happened as yet.

The Government's response to the consultation talks about serious crime and says that data

"is used in 95% of serious and organised crime prosecution cases handled by the Crown Prosecution Service Organised Crime Division, and has been used in every major Security Service counter-terrorism investigation over the last decade."

That is a fair point—95% is a high percentage—but in talking about the ruling it says that

"Member States can legislate for a regime which permits the targeted retention of communications data for the purpose of fighting serious crime, and the judgment sets out conditions that such legislation must satisfy in order to meet the requirements of EU law."

I hope the Minister can address this in his conclusion, but in terms of the definition of serious crime, the proposed subsections 60A, 61 and 61A outlined do not sufficiently limit acquisition of communications data for an "applicable crime purpose" to,

"the objective of fighting serious crime",

which is required in order to comply with the judgment in the case of Tele2 Sverige AB *v.* Post-och telestyrelsen and Secretary of State for the Home Department *v.* Tom Watson and Others. That is because the proposed section 86(2A) defines serious crime so broadly. The definition covers any crime by a body corporate; any offence

"which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy";

and any offence that carries a penalty of at least 12 months' imprisonment for offenders aged 18 or over.

Serious crime will be captured by the definition in proposed new section 86(2A); of course it will. However, the fact that an offence was committed by a body corporate or involves a communication or breach of privacy bears no relation to its seriousness and therefore takes us no further in limiting the acquisition of data to the objective of fighting serious crime. The minimum sentence definition will encompass the vast majority of criminal offences and apply regardless of the circumstances of the offence. In our opinion, the definition should be much narrower, taking into account the particular circumstances of the offence. The definition of serious crime should be met only when a person can reasonably expect to receive a sentence of significantly more than 12 months.

We opposed the 2016 Act's far-reaching bulk powers to acquire the personal and private data of our constituents; the regulations do not address our concerns. I appreciate that the UK Government have moved on the issue, having been forced to do so by the Watson ruling, but we would have welcomed their taking the opportunity to address our concerns via the regulations. Sadly, they have chosen not to do so. I am keen to hear the Minister's reply about the definition of serious crime.

4.41 pm

Ms Angela Eagle (Wallasey) (Lab): I have a few questions for the Minister about some of the matters that he set out. I would like a little more detail on them for the record, so that we can—I hope—go on to support the draft regulations.

These matters concern the delicate balance that must always exist between privacy and the need to fight crime by using material generated in the normal living of life, through new ways of communicating. Will the Minister say a little more about the balance that the Government have decided to strike in the draft regulations? Clearly the wide-ranging system under the existing legislation did not survive the jurisdiction of the Court, so the type of information that can be used for the purpose of fighting crime is being narrowed. How have the Government struck that new balance? I note that none of the draft regulations applies to national security, because it is not within EU competence. Does the regime now being established have any connection with issues of national security?

My second question is a more practical one about the independent authorisation of requests for information. We all agree that it is good to have independent oversight with the capacity to ensure that there is no drift and that the operational behaviour of the system stays within the

[Ms Angela Eagle]

reasonable bounds of the draft regulations. However, if serious crimes are being pursued, it is equally important that independent authorisation should not become a bureaucratic system that prevents our forces of law and order—which are already under huge pressure from Government expenditure cuts—from doing their job effectively and thereby lets serious criminals off the hook. Will the Minister say a little about the funding arrangements that will be implemented for the independent authorisation of requests, so that the system does not just become a big queue that prevents operational effectiveness in the police force?

Thirdly, does the Minister envisage any parliamentary oversight of the way that the system will evolve over time? Again, it is important to keep such things under review and ensure that they are working well. Clearly, the Home Affairs Committee may have some oversight, but does he envisage coming back to the House in any way?

Fourthly and finally, we are in a situation where Amazon, Facebook and a lot of the tech behemoths have more access to information about how we behave. Cambridge Analytica used 2,000 to 3,000 data points to analyse the likely voting behaviour of millions of people in the US presidential election and in the Brexit referendum in this country, as we know. Private and unaccountable corporations appear to have more access to information about individual citizens of our country than we allow the police. Does the Minister think that balance is right?

4.45 pm

Mr Wallace: I will first address the experienced points of the hon. Member for Wallasey. The balance between allowing our police forces to get on and do their job and bureaucracy is a challenge that the Home Office and Government have always faced. If there was a reason why we did not initially propose this type of independent authorisation, it was not some deep-state conspiracy theory, but the amount of bureaucracy we expect at a comms data level and whether that is proportionate to the police doing their job.

It is a difficult balance. Comms data is the norm. We are all wedded to our telephones—as I speak, some Members are wedded to theirs—and people conduct a serious amount of business, communication and crime on them, so that data will only increase. Comms data is not about the content, however; it is about the who, where and when, so it is at the lower level.

Subscription details—basically, which mobile telephone belongs to who and the billing address—are included in the regulations. The Court did not require us to do that, but we have put it into the independent authorisation, partly because law enforcement said, "Just get rid of the bureaucracy and hand it over to OCDA. We do not want to have it just for subscriptions and not others," and partly because it now fits that all these authorisations, whether they are the more intrusive bulk data and content intercept communications or not, are dealt with and oversighted independently.

That leads me to the points of the hon. Members for Wallasey and for Paisley and Renfrewshire North. The oversight will be independent. It will be accountable through the Investigatory Powers Commissioner, Lord Justice Fulford. He is also involved in the independent authorisation of the more intrusive areas of intercept and has an oversight role to look back at how the powers were used and whether they were proportionate and necessary. Funnily enough, within that, he can order disclosure to individuals if he feels that their data has been used wrongly. That goes some way to our venture—we have said to the European Court that there is already a form of notification in the system, which is that there are several opportunities for someone to be notified.

At the same time, there will be other scrutiny, such as an annual report by the Investigatory Powers Commissioner. The Intelligence and Security Committee will also be able to look at some of the more sensitive capabilities in detail. There is the Home Affairs Committee and the investigatory powers tribunal that individuals can take cases to if they feel that their data has been wrongly collected, wrongly stored or abused.

Without wandering too far off the regulations, I entirely agree with the hon. Lady's point about the private and public balance. We have a balance where if any of us in this room, or if I as a Minister, wants to do something, we need a warrant or authorisation with quite a lot of oversight, but if a private individual wants to park a car with a camera in it outside someone's house on a public highway, there is very little that person can do to stop them. If a large company wants to buy and sell someone's data or effectively surveil you and I, there is very little that we can do about it, Sir Graham. I worry that we go around in circles and that that goes pretty unchallenged by the law enforcement community. The General Data Protection Regulation is a good piece of work, which has sought to deal with that by bringing ownership of data back to individuals.

As the hon. Member for Paisley and Renfrewshire North said, we have drawn down the definition of "serious crime" to a crime with a sentence of one year or more. We have included some carve-outs below that, simply because most of those offences depend purely on comms data. For example, when investigating the persistent stalking or harassment of an individual, it is incredibly important to be able to use data about telephone behaviour, but the offence of stalking does not always meet that sentencing threshold—injunctions are often used, and so on. We therefore venture that that carve-out is important. Corporate manslaughter does not carry a custodial sentence, but I think we all believe comms data is really important in proving that a corporation or body failed in its duties or committed a criminal offence, which are often large in scale.

That is a pragmatic way of trying to keep people safe. The Court said it was up to the member state to define "serious crime"—it did not seek to do so itself. It is recognised that comms data is not as intrusive into our privacy as an intercept, which means that the serious crime threshold can be different from the three-year threshold that applies to the regime for more intrusive data collection.

On what the hon. Member for Torfaen said, we obviously told the Court that we would comply with its ruling about independent authorisation, but we have until April 2019 to set up independent authorisation on a scale that allows our police forces up and down the country to do their job. We have started recruiting and establishing a secure IT system—posts have been advertised and people are being interviewed for them. It is simply

set-up time. We cannot immediately rustle up that type of body. The OCDA will be answerable to the Investigatory Powers Commissioner and based throughout the United Kingdom. It will obviously spend a lot of its time liaising with police forces, because it will make direct requests via the single point of contact—the expert—in each force.

The Court accepts that, and it is really important that we deliver to that timetable. I have asked for an update every two weeks on how we are progressing. The Court recognises that we actually have to deliver—it cannot just immediately rule everything illegal, because the system would in effect fall over. The Court gave us time, and it has recognised our ability to do that.

The Court ruling on which the draft regulations are based considered five arguments. In two cases—independent authorisation and the serious crime threshold—the Court found that our law was unlawful and needed to be changed. We have addressed that. In the other three cases, the Court did not find in the plaintiff's favour or make a ruling. For example, it did not find that our retention was "general and indiscriminate". That is why we are dealing with comms data. The hon. Member for Paisley and Renfrewshire North referred to bulk data. The draft regulations focus specifically on the comms data regime, as requested.

I hope I have answered hon. Members' questions. We are in a good position. I am entirely comfortable that independence will be used in the authorisation process. We have not popped some conspiracy—this is a perfectly functional thing. At the moment, the Home Office is funding the set-up of OCDA, alongside the Investigatory Powers Commissioner. I recognise the pressure on resources for police forces. I have to do my best to ensure that that body is as minimally bureaucratic as possible but does the job of giving assurances that people's data is dealt with independently and not abused.

Question put and agreed to.

4.55 pm

Committee rose.