Vol. 774
No. 48

Wednesday
19 October 2016

PARLIAMENTARY DEBATES
(HANSARD)

HOUSE OF LORDS

OFFICIAL REPORT

ORDER OF BUSINESS

Lords wishing to be supplied with these Daily Reports should give notice to this effect to the Printed Paper Office.

No proofs of Daily Reports are provided. Corrections for the bound volume which Lords wish to suggest to the report of their speeches should be clearly indicated in a copy of the Daily Report, which, with the column numbers concerned shown on the front cover, should be sent to the Editor of Debates, House of Lords, within 14 days of the date of the Daily Report.

This issue of the Official Report is also available on the Internet at
https://hansard.parliament.uk/lords/2016-10-19

The first time a Member speaks to a new piece of parliamentary business, the following abbreviations are used to show their party affiliation:

Abbreviation	Party/Group
CB	Cross Bench
Con	Conservative
DUP	Democratic Unionist Party
GP	Green Party
Ind Lab	Independent Labour
Ind LD	Independent Liberal Democrat
Ind SD	Independent Social Democrat
Ind UU	Independent Ulster Unionist
Lab	Labour
LD	Liberal Democrat
LD Ind	Liberal Democrat Independent
Non-afl	Non-affiliated
PC	Plaid Cymru
UKIP	UK Independence Party
UUP	Ulster Unionist Party

No party affiliation is given for Members serving the House in a formal capacity, the Lords spiritual, Members on leave of absence or Members who are otherwise disqualified from sitting in the House.

House of Lords

Wednesday 19 October 2016

3 pm

Prayers—read by the Lord Bishop of Chester.

Short-Term Letting: Deregulation

Question

3.06 pm

Asked by ***Baroness Gardner of Parkes***

To ask Her Majesty's Government what steps they are taking to address the impact on long-term residential rental properties in London of the deregulation of short-term letting last year.

Baroness Gardner of Parkes (Con): My Lords, while reminding the House of my interests as declared in the register, I beg leave to ask the Question standing in my name on the Order Paper.

The Parliamentary Under-Secretary of State, Department for Communities and Local Government and Wales Office (Lord Bourne of Aberystwyth) (Con): The Government support the shared economy and monitor trends in private rented housing through the English housing survey. It is right that Londoners should have similar rights as elsewhere in England and be free to sublet their homes where their tenancy, contract or mortgage allows. We do not support the abuse of planning laws, and those in breach face a fine of up to £20,000.

Baroness Gardner of Parkes: I thank the Minister for that Answer but, in view of the report in today's press that Gavin Barwell has just announced a clampdown on rogue landlords and a return of powers to local councils to enable them to deal with crowding in residential lettings, will the Minister confirm that the licensing powers for local councils will also cover Airbnb lettings, which I have reported to the House on a number of occasions, whereby 10 people are routinely occupying one-bedroom flats in some residential blocks for a series of short lets that are not allowed under those leases?

Lord Bourne of Aberystwyth: My Lords, I think that to a degree my noble friend has covered the issue with her last point. Powers already exist for landlords to enforce provisions if they are in breach of leases. There are also planning regulations. The mandatory listing changes in relation to HMOs announced yesterday in another place by Gavin Barwell relate to residences where there are shared facilities. That would not cover tower blocks, which I think is the area on which my noble friend is focusing her attention.

Baroness Boothroyd (CB): My Lords, since councils lost the powers of licensing short lets last year, is it correct that the only recourse that other residents in a block have in cases of threatening behaviour or damage to the property is to call the police?

Lord Bourne of Aberystwyth: My Lords, that is not the case. There are powers in relation to London. This is only a London issue, too; elsewhere in the country, prior to the change in the Deregulation Act 2015, there was a power to let without limitation. In London there is now a power to let for up to 90 consecutive days, so anything in breach of that is a breach of planning law and it rests with the local authority to enforce it. As I have indicated, there are provisions in leases. There are also of course provisions in relation to statutory nuisance; if litter should be left around or should there be noise, there are existing powers. I do not think we need additional ones.

Baroness Donaghy (Lab): My Lords, what assurance can the Minister give the House that the Government are looking carefully at the health and safety, fire prevention and noise and nuisance aspects of short lets? They seem to be using not very satisfactory existing law instead of looking at the situation as a whole. Can he assure us that the Government have a picture of this developing situation?

Lord Bourne of Aberystwyth: My Lords, the noble Baroness refers to an issue that is London-only, because prior to the change in the Deregulation Act, the position was exactly the same in other areas of England. The recent change in the law brought London to a degree in line with the rest of the country, except that there are more restrictions in London, because there is a 90-day limit. As I said to the noble Baroness, Lady Boothroyd, existing powers on statutory nuisance are and have always been available to other tenants and landlords. Of course we monitor the situation, but there is already a satisfactory range of powers.

Baroness Eaton (Con): My Lords, if short lets such as Airbnb usage become a full-time use of residential property, I believe that it then becomes business usage. Can my noble friend confirm that planning permission is required in such cases?

Lord Bourne of Aberystwyth: My Lords, as I said, there is an existing power. In relation to the change of law in London, if a let exceeds 90 consecutive days, it requires a planning use change. If there is a total change of user, it would also require planning permission under existing law. Also, as I said, powers exist in many leases. Recently, in the so-called Nemcova case in the London Borough of Enfield, a landlord enforced provisions in a lease in just such a situation.

Lord Tope (LD): My Lords, is the Minister aware that according to the Inside Airbnb website, a total of 42,646 properties are listed in London alone? Is he further aware of those 42,646, 17,593 are multiple listings—in other words, the host manages numerous properties? Does he agree that hosts with multiple listings are more likely to be running a business, unlikely to be living in the property—certainly not all of them at the same time—and potentially in violation of the Deregulation Act's 90-day limit on short-term lettings? Do the Government really think this is satisfactory? If not, what more are they going to do about it?

Lord Bourne of Aberystwyth: My Lords, as the noble Lord said, if it is in excess of the 90-day limit in London, it is in breach of the law. Powers exist with local authorities to enforce that: it is for local authorities to do so as the power rests with them. In addition, as I mentioned, a case came into the department today of a landlord saying to a tenant, "You are in breach of the law. Please take down this listing: it would be a breach of your lease". The combination of those two things—the power in the contract or lease to enforce a particular provision and the existing powers of local authorities—should meet the cases to which the noble Lord refers.

Baroness Finlay of Llandaff (CB): In light of the previous question about the safety of tenants, can the Minister clarify whether the Gas Safety (Installation and Use) Regulations 1998 apply to landlords with such short-term rental properties and how such regulations can be enforced to prevent carbon monoxide poisoning among residents in places where the gas appliances are old and unsafe?

Lord Bourne of Aberystwyth: I will have to write the noble Baroness on that rather technical issue. It is an important issue but I have no knowledge of that and would not want to mislead her, so I will reply to her in writing and ensure that a copy is placed in the Library.

Lord Kennedy of Southwark (Lab): My Lords, at the very least, the Government should take action to ensure that holiday letting company websites are checking that houses on their sites are genuine lets of less than 90 days. Otherwise, there is a risk that statutory regulation, safety requirements and insurance provisions are not being complied with.

Lord Bourne of Aberystwyth: My Lords, that was an exhortation to the Government. As I said, the power lies with local authorities. There are things that the Government should be doing—I would be the first to admit that—but this rests with local authorities and I encourage them to do that. That is the position under the Deregulation Act. It is also a responsibility of landlords to ensure that the terms of the lease are adhered to. This is not a direct responsibility of the Government. We ensure that councils have the proper powers and landlords have the facility to go to court, but the responsibility rests with local authorities and landlords.

Lord Naseby (Con): I speak as a former chairman of the London Borough of Islington's housing committee. Does my noble friend recollect the Rachman period and De Lusignan? Against that background, does a local authority today have the legal right to check the status of any property? If, as many of us believe, the worst rogue landlords do not admit to being landlords at all, who has the authority to investigate these situations?

Lord Bourne of Aberystwyth: My Lords, I was still at junior school in the Rachman period, so I have only a vague recollection of it. From the noble Lord's experience in Islington and since, he is aware of the situation in dealing with rogue landlords and others. We are very keen to do that, which is exactly why yesterday Gavin Barwell in another place announced regulations, which we are consulting on. It is important that we do, as I have indicated, give the proper powers to local authorities as we have done and say, "This is a matter for you".

International Development Aid

Question

3.15 pm

Asked by ***Baroness Kennedy of Cradley***

To ask Her Majesty's Government what are their priorities for the United Kingdom's international development aid budget.

Baroness Kennedy of Cradley (Lab): My Lords, I beg leave to ask the Question standing in my name on the Order Paper. In doing so, I declare an interest as a patron of Action on Poverty.

Baroness Mobarik (Con): The UK's aid budget will be delivered according to the objectives in the UK aid strategy—namely, strengthening global peace, security and governance; strengthening resilience and response to crises; promoting global prosperity; and tackling extreme poverty and helping the world's most vulnerable. This approach builds on the strong successes of the last five years and recognises the need to ensure that everything we do contributes to the national interest.

Baroness Kennedy of Cradley: My Lords, I thank the Minister for that reply. I think that Members on all sides of the House are increasingly concerned about the Government's dogmatic approach to using the aid budget to promote private healthcare services in developing countries. How much has DfID contributed to private health initiatives such as private fee-paying hospitals, and how does this meet the objective of building sustainable, universal healthcare systems that can deal with humanitarian emergencies such as Ebola?

Baroness Mobarik: My Lords, the UK provides technical assistance and financial support focused on helping countries to strengthen their whole health system. This Government remain committed to delivering on our international commitments, including the global goals, and therefore strongly support progress towards global goal 3, which is about good health and well-being. For example, we have supported Sierra Leone over the course of the crisis to establish systems that can rapidly detect and contain outbreaks of Ebola, and so on, before they grow into epidemics. We are working with the Government and the World Health Organization as well as other partners to make those systems resilient and enduring.

Lord Lawson of Blaby (Con): My Lords, since the single most important factor in determining the success of development in developing countries is the quality of leadership in those countries, would my noble friend ask her department to consider whether the best use of its burgeoning budget might not be to provide scholarships for the leaders of the future from the developing countries to study at our excellent universities?

Baroness Mobarik: Governance aid is a major part of our strategy to provide good governance in countries around the world that we are trying to help. If the noble Lord is alluding to fraud and corruption, I just want to say that the Government do not tolerate corruption or misuse of taxpayers' funds in any form. When DfID identifies issues relating to fraud, it takes them very seriously and investigates them thoroughly.

Lord Crisp (CB): My Lords, I take it from the noble Baroness's reply that the priorities include working towards achieving the sustainable development goals, which, as she knows, include achieving universal health coverage globally. Will she agree with me that universal health coverage will not be achieved without strengthening the role that nurses can play, and would she further agree that the UK, working with the Commonwealth and the World Health Organization, can play a major role in raising the profile of nursing globally and ensuring that the potential of nurses to do even more is understood and acted on?

Baroness Mobarik: I thank the noble Lord for his question, and I commend him on his work with the APPG on Global Health. We welcome the overall findings of the *Triple Impact* report on nursing and are committed not only to training new nurses but to improving the skills of nurses already deployed. We support an array of health professionals, embracing a whole-system approach which is aligned with country priorities. For example, the Health Partnership Scheme supports UK health professionals to volunteer to build health workforce capacity in around 30 developing countries.

Lord Purvis of Tweed (LD): My Lords, the Minister will be well aware of the overwhelming consensus in this House in 2015 during passage of the international development Act, on which I had the privilege to be the Member in charge. The House should also be very proud that in the 2016 Aid Transparency Index, the UK was the leading country in the world for aid transparency. Was the Minister therefore not as surprised as I was to read in the *Mail on Sunday* of 9 October the following words attributed to Priti Patel, the Secretary of State:

"I'll defy order to blow £12 billion on foreign aid"?

The article continued:

"International Development Secretary told aides she'll ignore requirement".

Will this Government act within not only the word but the spirit of the law, and will they not only meet their international obligation year on year but work with our friends and colleagues in countries around the world who do not meet theirs? We should be leading by example, not by such damaging and inconsistent headlines in the *Mail on Sunday*.

Baroness Mobarik: I thank the noble Lord for his question. I think we are leading by example. We are meeting the 0.7% target, which is a manifesto commitment. It is enshrined in law. My right honourable friend the Secretary of State has been unequivocal that we will continue to honour that promise.

Lord Anderson of Swansea (Lab): My Lords, will the Government continue to support the OECD definition of what spending constitutes foreign aid?

Baroness Mobarik: I shall write to the noble Lord.

Baroness Kinnock of Holyhead (Lab): My Lords, is the Minister aware that DfID's Secretary of State has advocated the abolition of that very department, given what she calls the waste of development funds, and that by 2020 she will accept a 44% increase in the proportion of development assistance spent by departments other than DfID? Does the Minister think that such a Secretary of State has the personal and political commitment necessary to properly decide development priorities?

Baroness Mobarik: Yes.

British Servicemen: Vexatious Law Suits

Question

3.22 pm

Asked by ***Lord Touhig***

To ask Her Majesty's Government what steps they are taking to prevent vexatious law suits being brought against British servicemen.

The Minister of State, Ministry of Defence (Earl Howe) (Con): My Lords, the Prime Minister has recently reaffirmed that the Government will put an end to the industry of vexatious claims. As a first step, we have already announced that the Government intend to derogate from the relevant articles of the European Convention on Human Rights in future conflicts whenever that is considered appropriate. We hope to announce further measures shortly.

Lord Touhig (Lab): At the last election, the Conservative manifesto promised that our Armed Forces would not be subject to "persistent" legal claims that,

"undermine their ability to do their job".

As the Minister said, the Prime Minister said in her conference speech that,

"we will never again in any future conflict",

allow Britain's Armed Forces to be harassed. However, the Defence Secretary contradicted her in a statement last week when he said that we will act to stop such claims only where this is appropriate. Our forces are subject to UK service law and allegations of criminal activity are rightly investigated. However, under this Government a whole industry of vexatious allegations against the men and women of our Armed Forces has flourished. So will the Minister tell us: is the Government's policy the one set out by the Prime Minister or the one set out by the Defence Secretary?

Earl Howe: My Lords, there is no contradiction. As the noble Lord rightly said, the vast majority of service personnel deployed on operations overseas have acted in accordance with the law and their training. However, where credible criminal allegations are made, we must investigate in accordance with our legal obligations.

[Earl Howe]
What we need to do is strip out the vexatious claims. That is why we are taking a range of measures, as I am sure the noble Lord is aware.

Lord Craig of Radley (CB): My Lords, what combat immunity or other legal protection have the Government arranged for Armed Forces personnel currently engaged in armed conflict in the air or on the ground, in the light of the views expressed by the Prime Minister?

Earl Howe: As regards combat immunity, the Government have previously made it clear that we will not rule out legislating, which is being considered among a range of options. It has been suggested that we should simply reinstate Section 10 of the Crown Proceedings Act; that is one of the options we are looking at, but it would be possible only under certain specific circumstances. No plans are in train for any immediate change on that front.

Lord Thomas of Gresford (LD): My Lords, I have professional experience of fraudulent claims and of legitimate claims like the Baha Mousa case, where the deceased received 95 injuries before he died. I note that the Ministry of Defence has settled 326 claims at a cost of £32 million; I assume that those were legitimate claims. Do the Government now intend to abolish or prevent all claims being brought by prisoners or civilians who are injured in the course of operations, regardless of whether they are legitimate or vexatious?

Earl Howe: As the noble Lord is aware, the Iraq Historic Allegations Team looks into these allegations, which have totalled more than 3,300 to date. The current case load is around 1,600 and it expects to reduce that number to 250 by next January. We cannot simply close it down, because that would mean leaving these allegations open to referral to the International Criminal Court in The Hague, with the possibility of trials there. We must therefore investigate properly in this country.

Lord Faulks (Con): My Lords, of course it is absolutely right that all our troops should be subject to international humanitarian law. My noble friend has described the first step the Government have taken. I suggest two further steps: putting combat immunity on a firm statutory basis, as the noble and gallant Lord suggested—there is far too ambiguity about its scope—and considering restricting the territorial scope of the Human Rights Act, which it was once thought clearly applied only within the United Kingdom.

Earl Howe: I am grateful to my noble friend. The proposal he makes is being looked at. We have no current plan to amend the Human Rights Act. As and when a British Bill of Rights is presented to Parliament, this is no doubt a matter that can be debated in that context.

Lord West of Spithead (Lab): My Lords, can the noble Earl say why ex-military are treated in a different way in Northern Ireland when it comes to investigation of historic crimes? Surely there is a requirement to look on an equal basis at all these cases, be it a legacy case that includes the military or some other person within Northern Ireland. Why are they treated differently?

Earl Howe: My Lords, we are acutely mindful of the impact of any allegations against service personnel, particularly veterans and their families. Where veterans are involved in processes that arise out of alleged actions during their service, we will provide legal support as necessary—regardless of the length of an individual's service or the time that has elapsed since the events occurred. It is always possible for us to look at improving the way we support veterans—and indeed serving personnel—and we are happy to look at anything in that area.

Lord Robathan (Con): But my Lords, is not the PSNI legacy unit pursuing soldiers who committed acts 41 years ago, the cases against whom have been dismissed on at least two occasions? This means that people in their 70s are being arrested and charged, yet the other people who were in their patrol are already dead and cannot give evidence for them.

Earl Howe: My noble friend makes a powerful point. We want to process expeditiously any such cases where there is credible evidence. That is why we are supporting the creation of the historical investigations unit, which will roll into one some of the functions of the ombudsman and the Police Service of Northern Ireland and create efficiencies in the process. The life of that body will be limited to five years, which should provide some assurance that cases will not be allowed to drag on.

Calais Camps: Unaccompanied Minors

Question

3.29 pm

Asked by ***Lord Roberts of Llandudno***

To ask Her Majesty's Government, in the light of the planned demolition of the refugee camps in Calais by 31 October, what steps they are taking to ensure that all unaccompanied minors are registered and considered for settlement in the United Kingdom before that date.

The Minister of State, Home Office (Baroness Williams of Trafford) (Con): No date for completing the demolition of the camps has been specified. However, Home Office teams have been deployed to France to speed up the identification process. We will transfer as many as possible of the children who qualify under the Dublin regulations before the start of the clearance, and in the coming weeks we will start to transfer other unaccompanied refugee children under Section 67 of the Immigration Act 2016.

Lord Roberts of Llandudno (LD): I thank the Minister for that Answer. I am sure we all welcome the 14 children who were received here two or three days ago, but I am told that that currently leaves 1,020 unaccompanied children in Calais. Fourteen have come here, so there are only 1,006 left to accommodate. Is there a plan to ensure that every one of those 1,006 will be registered and given the opportunity to apply to enter the UK under the Dubs amendment? With the coming winter, surely we cannot leave any children open to exploitation, hunger and homelessness when we have the opportunity to fulfil their needs.

Baroness Williams of Trafford: It is estimated that there are approximately 1,300 children in the camps in Calais and that about a third of that number may be eligible to come here under either Dubs or Dublin. As I have said to the House on previous occasions, since the beginning of the year 140 children have qualified under the Dublin regulations and most of them have been transferred. In addition, this week 14 children were transferred on Monday, 13 on Tuesday and 12 today, so the actual number is estimated to be around three times the number that the noble Lord has stated. However, whether under Dubs or Dublin, we are absolutely determined to get those children here. The noble Lord will know—because I have stated it previously—that the Home Secretary regularly presses for those children, first, to be brought here and, secondly, if they are not here, to be put in places of safety before the camp is cleared.

Baroness Gardner of Parkes (Con): My Lords, a lot of dissatisfaction has been expressed in the paper today with people saying that these are adults rather than children. The paper went on to say that the best way of identifying age is through a dental examination, as wisdom teeth are highly significant, and that is why I am asking this question. It also said that a dental examination could not be done without parental consent, although of course various X-rays can be done without even opening a child's mouth. There is something very strange about that. I wonder why it has not been possible to come to an agreement whereby, if you want to come in, you are obliged to give consent to be checked regarding your age.

Baroness Williams of Trafford: My Lords, I confess to being 49 years of age and still not having wisdom teeth, but that probably says something about me. We are working very closely with the French authorities and their partner agencies to ensure that all those who come to the UK from the camps are eligible under the Dublin regulations. All individuals referred to the UK authorities by the FTDA are interviewed by French and UK officials and, where credible and clear documentary evidence of age is not available, criteria including physical appearance and demeanour are used as part of the interview process to assess age. That is the process in France and I want noble Lords to be quite clear that we are bound by the French system of assessing age in France. When those children come to the UK, we do not use dental X-rays to confirm the ages of those seeking asylum. The British Dental Association is vigorously opposed to them and has described them as inaccurate, inappropriate and unethical.

Lord Clinton-Davis (Lab): Will the Minister assure the House that no minors are being treated illiberally or will be in the future?

Baroness Williams of Trafford: The noble Lord is absolutely right to ask that. We are primarily seeking to ensure that no minor is made more vulnerable in France, and that when they come here they are properly looked after in accordance with the safeguarding laws in this country, which are very stringent. That is exactly what we seek to do.

Lord Hylton (CB): The Minister will correct me if I am wrong, but my understanding is that there is only one British official permanently in Calais for liaison with the French authorities, and only one official of the UN High Commissioner for Refugees. Surely that is inadequate, and surely the need for competent interpreters must be properly addressed. Does the Minister agree?

Baroness Williams of Trafford: What I can agree is that the number of officials in France is changing in accordance with the numbers needed in various roles. We have a permanent dedicated Dublin unit in the Home Office. In addition, on Monday, we sent nine officials to France to assist. I repeat again: we are guided by the French and by French law; we cannot do any more than that. We would not seek to usurp French law in trying to make the situation better for those children who we seek to help.

Lord Dubs (Lab): May I do something that I do not think I have ever done before and welcome what the Government have said today? It is good news that child refugees are coming to Britain. I wish that we had had these statements several months ago, but it is happening now. I simply ask the Minister to assure us that all pressure is being brought to bear on the French Government, because I understand that they have a part to play in assessing the other children who come under the Immigration Act.

Baroness Williams of Trafford: I thank the noble Lord for his words and for the time that we spend regularly now speaking to each other about the situation in Calais and elsewhere in Europe. Not only is every pressure being brought to bear, but we are trying very hard to work with the French and not against French law.

Pension Schemes Bill [HL]

First Reading

3.37 pm

A Bill to make provision about pension schemes.

The Bill was introduced by Lord Freud, read a first time and ordered to be printed.

Pensions: Sale of Annuities

Statement

3.37 pm

Lord Young of Cookham (Con): My Lords, with the leave of the House, I shall now repeat as a Statement the response to an Urgent Question given in the other place by Simon Kirby, Economic Secretary to the Treasury. The Statement is as follows:

"Mr Speaker, this Government have taken a great step forward in giving more and more people freedom over how they choose to use their pension savings when they retire. We have, in fact, already seen over 300,000 people choosing to access their pension flexibly since the reforms were introduced.

Alongside our efforts to do this, we also said that we would look at how we could spread this flexibility to people locked into existing annuities. We consulted

[LORD YOUNG OF COOKHAM]
extensively with the industry and with consumer groups to explore whether we could put in place the right conditions for a market to develop that could facilitate this. Throughout our investigations, one of our very highest priorities was to establish whether people would be able to get a good deal through such a market. But in the course of our efforts to investigate the viability of a secondary market in annuities, two things became clear. First, without compromising on consumer protections, there would be insufficient purchasers of these annuities to create a competitive market in which British pensioners could get a good deal. Secondly, pensioners trying to sell their annuities would also be likely to incur high costs in doing so.

This Government have made it very clear that we want this to be a country that works for everyone. That includes making sure that everyone gets a high level of consumer protection. It has become clear now, through our extensive research, that a secondary market would not be able to offer this. Rather than being to the benefit of British pensioners, it would instead be to their detriment, and for this reason, we are not prepared to allow such a market to develop and we will not be taking this policy forward".

3.40 pm

Lord McKenzie of Luton (Lab): My Lords, I thank the Minister for repeating the Statement, but this is the second government U-turn on pension-related matters that we have seen in the space of just a few weeks—another example of a flawed approach to pension policy characterised by fanfare announcement, a period of rethink and then a retraction by press release. In this case, there has been an abandonment of plans for a secondary annuities market, as we have heard, which was never credible without consumer detriment.

At a time when we need to build confidence and sustainability in our pension system, what sort of message does this chaotic approach send to those we should be encouraging to save more for their retirement? How do the Government propose to address the £960 million additional black hole in their finances that now arises from the reduction in their projected tax revenues?

Lord Young of Cookham: I am grateful to the noble Lord for his measured response. On the first question, I do not think confidence in pensions would be enhanced if we went ahead with the scheme without adequate consumer protection. Against a background over the past 20 or 30 years of financial products being sold incorrectly, it would have been quite wrong to go ahead with this scheme. As I said, it was unlikely that a vibrant and competitive market would emerge and we could not get the market to work without undermining consumer protections.

On the figure pencilled into the Government's accounts, had the policy gone ahead, it would have brought forward a certain number of tax receipts into the early years at the expense of getting those receipts in the later years. Overall, I think it will be neutral. It will be up to the Chancellor in his Autumn Statement to explain how the books will be balanced.

Lord Stoneham of Droxford (LD): Well, well, well, my Lords, what has happened to the party of freedom and freedom of choice? The Government promised us stability in the general election. That was lost by the referendum result. They promised us an economic plan, which is now in shreds. Page 3 of their manifesto said that the Conservatives would,

"give you the freedom to use your pension savings as you want".

No. Now they will not.

There was a flagship announcement by George Osborne in March 2015 of another government initiative. It had a good headline, and a total lack of follow-through once Steve Webb, the Pensions Minister, was no longer in government. Therefore, inevitably, the Government are left abandoning it. People are locked into poor-performing annuities and they deserve an escape route. I have four questions for the Minister.

How are people being informed of this change, particularly those who would like to get out of their locked-in annuity policies? What help will the Government give to people locked into these poor performing annuities? Is this reversal due to the low interest rates following Brexit totally destroying the returns on lump-sum annuities? Finally, by making this announcement outside Parliament, is this another example of the Government not being in control of what they are doing and economic and pension policy being dictated by the markets?

Lord Young of Cookham: I am grateful to the noble Lord. On the timing of the announcement, sometimes the market-sensitive nature of an announcement means it has to take place at a specific time, quite often when the Stock Exchange is not open. So far as those who are disappointed are concerned, the information available to the Government is that only 5% of those with annuities would be likely to have taken up this offer had it gone ahead, so roughly 95% will not be affected by the announcement. It is independent of any level of interest rates; it is not a function of quantitative easing or anything like that. I see that Steve Webb, to whom the noble Lord referred, has said that the decision is "disappointing" but "understandable", implying that he goes along with it.

The final point about information is a good one and I will see what we can do to let people know. I suspect that many will have read the newspapers and are aware that this option will no longer be available.

Lord Hain (Lab): Is not the problem that the Government have failed all along to provide a properly regulated, publicly controlled vehicle to satisfy the needs of those with very small annuities—often, by the way, ones that do not provide protection either for spouses or against inflation—who want to exchange them for a cash sum that they can repay debts with or provide for their partners? Now we have the worst of both worlds, being stuck in this policy impasse.

Lord Young of Cookham: I think the noble Lord is suggesting that, rather than the private sector providing an option for these annuitants, the Government should have provided it. That was never the proposal and he will know that, along with the other pension freedoms,

they are operated by the private sector. Those who opt out of their pension to use the other options do so without resorting to a government scheme.

Lord Tugendhat (Con): My Lords, I congratulate the Government on reversing a bad policy, on doing so both quickly and courageously, and on the clarity with which the Minister has justified it. The points he has made demonstrate clearly that the decision that has now been taken is the right one and that it is always better to learn from experience, so Governments should be congratulated when they do so.

Lord Young of Cookham: I am enormously grateful to my noble friend, who has good knowledge of the workings of the City. As he implied, it has become increasingly clear that creating the conditions that will allow a vibrant and competitive market to emerge, with multiple buyers and multiple sellers of annuities, could not be balanced or achieved without sufficient consumer protection. After having drilled down and consulted regulators, consumer organisations and other stakeholders, the Government have come to the conclusion that it would not be in consumers' interests to continue with this policy.

Baroness Drake (Lab): I agree with the Government's decision and I believe that the Chancellor has called time on a bad policy. I feel it now and I certainly believed it when it was put. The risk to annuity holders of trading in a secondary annuity market are extremely high and the complicated regulatory requirements to protect them in such a market would undoubtedly mean that the costs would have been transferred to the consumer. It was also evident that there would be insufficient purchasing in that market. All these issues were raised by my noble friend Lord McKenzie, other noble Lords and me when this enabling legislation was debated. It was clear what the problems were but the Government were determined to push ahead. Why did the Government put enabling legislation in place before they had satisfied themselves that the creation of a secondary annuity market was a viable policy, when it was absolutely evident that all the problems which have now been deployed for not proceeding with a secondary annuity market existed then and people articulated them very clearly? That is the problem. It was clear that the secondary annuity market would not work, so why was enabling legislation rushed through?

Lord Young of Cookham: In all seriousness, I commend the noble Baroness on her foresight in being able to see in March 2015 that this was not a runner. That was not the view of many financial commentators at the time. It was seen to be consistent with those who had not yet reached retirement age and therefore had the freedom not to have an annuity. It was seen to be right to extend that freedom to those who had already purchased an annuity. In principle, it was the right thing to explore but, as I said in response to my noble friend, as we drilled down it became clear that there was not the secondary market that was necessary. Moreover, those who were going to sell their annuities would have had to have a medical examination, they would have had to pay brokerage charges and they would probably have faced administrative costs. It would have reached only a relatively small percentage. For all the reasons she has given, we have come to the same conclusion as the noble Baroness, albeit a little after her.

Lord Naseby (Con): My Lords, I declare an interest as a trustee of the Parliamentary Contributory Pension Fund; I should make it clear that you cannot have an annuity through that fund. Nevertheless, is not the core of the issue that a number of commentators have rubbished current annuities but that, in any case, no one knows exactly how long anyone will live, and that at some point your annuity will pay back quite handsomely regardless of what its level may be? Against that background, it seems to have been absolutely right for Her Majesty's Government to do another analysis now, in a changing situation, and to decide that what was said more than a year ago is not correct today. Given that, I would have hoped that Her Majesty's Government would think again and I congratulate them on doing so.

Lord Young of Cookham: I am grateful to my noble friend for his robust support for the decision that has just been taken. Of course, even had we gone ahead with the policy, a huge number of those with annuities would have been better off sticking with them rather than trading them in, for the reasons that we have heard.

Investigatory Powers Bill

Report (3rd Day)

3.50 pm

Clause 137: Modification of warrants

Amendment 180

Moved by ***Lord Keen of Elie***

180: Clause 137, page 110, line 4, leave out subsection (6)

The Advocate-General for Scotland (Lord Keen of Elie) (Con): My Lords, Amendments 180, 181, 197, 198, 205, 206, 231 and 232 relate to judicial commissioner approval of major modifications to warrants issued under Parts 6 and 7 of the Bill. They seek to provide additional clarity regarding the matters the commissioner must review when deciding whether to approve such a modification.

The Bill already provides for major modifications to such warrants. In the context of bulk interception, bulk acquisition and bulk personal dataset warrants, a major modification may be used to add or vary one of the operational purposes for which data may be examined under the warrant. As regards bulk equipment interference warrants, a major modification can additionally add to or vary any description of conduct in the warrant.

The Bill requires full double-lock authorisation from a Secretary of State and a judicial commissioner for any major modification to a bulk warrant. These amendments will not change that. Instead, they provide greater clarity about the matters that a commissioner must consider when determining whether to approve a modification to a bulk warrant.

[Lord Keen of Elie]

The amendments specify that, for major modifications to add or vary an "operational purpose", a judicial commissioner must review the Secretary of State's conclusions as to whether the modification is necessary, applying the same principles as would be applied by a court on an application for judicial review and ensuring that the commissioner complies with the duties in relation to privacy set out in Clause 2, the so-called privacy clause.

In the context of bulk equipment interference, if a major modification proposes to add or vary a description of conduct, the judicial commissioner must also review the Secretary of State's conclusions as to whether the conduct authorised by the modification is proportionate to what is sought to be achieved by it. The amendments are intended to ensure clarity and consistency across the Bill, and as such are to be welcomed.

The sharing of data and intelligence with our overseas partners is critical to the work of our security and intelligence agencies. Without working together with our allies, those agencies could not do their vital work of keeping us safe. Amendments 184, 185, 201, 202, 209 and 210 simply clarify the consideration that must be given by the Secretary of State before authorising the disclosure to overseas authorities of data acquired under the bulk powers in the Bill.

The Bill already places a duty on the Secretary of State to consider whether corresponding safeguards will be applied to the data that are to be shared with the overseas authority in relation to their retention and disclosure. These amendments make explicit that the Secretary of State must be satisfied that the overseas authority has in place safeguards, to the extent appropriate, that correspond to those in the Bill not only in respect of the retention and disclosure of the data shared in bulk but in relation to their selection for examination. This group of amendments therefore makes absolutely clear that proper consideration will be given to the examination safeguards that are applied whenever bulk data are shared with another country. I beg to move.

Baroness Hayter of Kentish Town (Lab): My Lords, I thank the Minister for moving these amendments, all of which we are happy to support and some of which respond to concerns we raised in Committee.

It may assist the House if I outline at this stage the purpose of Amendment 185A, in the names of my noble friend Lord Rosser and myself, which is about safeguards for disclosing overseas-related material for our foreign allies and agencies. That is material, possibly including information sent overseas by UK residents, obtained by our security and intelligence services under bulk interception warrants. It is an amendment which we hope the Government will feel able to accept.

In Clause 142, before any information obtained under a bulk interception warrant is disclosed overseas, the Secretary of State must ensure that arrangements and safeguards are in place regarding the retention and disclosure of such material, as the Minister has outlined. These requirements correspond to Clause 141 safeguards for domestic arrangements: that is, requiring that the number of people to whom the bulk-intercepted material is disclosed, the extent of disclosure and the number of copies made is limited to the minimum necessary. These safeguards also require the destruction of such material where there are no longer grounds for retaining it.

However, unlike Clause 141 for domestic arrangements, Clause 142 for overseas disclosure provides a wide discretion for the Secretary of State, whereby she or he must ensure equivalent safeguards only,

"to such extent (if any) as the Secretary of State considers appropriate".

It could, therefore, be possible for the Secretary of State to decide that no safeguards are required in a particular case.

We recognise absolutely that the UK will need to share intelligence with overseas agencies and our amendment does not undermine the ability of UK agencies to do that. We also accept that overseas disclosure may be of a different nature, with particular political, diplomatic or security implications, all of which the Secretary of State must consider. However, the present wording is surely too wide and, if I have understood it correctly, would not be subject to subsequent review. Amendment 185A removes this very broad discretion and requires that it must appear to the Secretary of State that safeguards corresponding to the requirements under Clause 141(2) and (5) will apply in relation to disclosure overseas.

The Minister will not be surprised if I make reference to the Szabó v Hungary finding that minimum standards should be set out in law to avoid abuses of power and that,

"it would be contrary to the rule of law … for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power".

The judgment notes that,

"the law must indicate the scope of any such discretion … with sufficient clarity … to give … adequate protection against arbitrary interference".

I hope that the Government will feel able to accept the amendment as, if anything, extra safeguards may, indeed, be required where sensitive information is being disclosed abroad. We look forward to the Minister's response on this.

Baroness Hamwee (LD): My Lords, we, too, are happy with the government amendments in this group and we support Amendment 185A. The issue is about the discretion in the application of Clauses 141(2) and 141(5)—and, shortly, Clause 143—not their relevance. The term "appropriate" suggests to me a degree of discretion which may not be related to relevance. The term "mutatis mutandis" is not one commonly used in legislation, I think, but it is that provision that one wants to see—only changing what is necessary to be changed. I do not know the proper way of dealing with that, but "appropriate" seems to be inappropriate in the context.

4 pm

Lord Keen of Elie: My Lords, as the noble Baroness, Lady Hayter, has observed, Amendment 185A would remove the Secretary of State's discretion to consider the extent to which the application of corresponding safeguards is appropriate in relation to the sharing with an overseas authority. The Government consider

that this is a vital provision and its removal from the Bill would pose a real risk to the national security of this country and other countries around the world. The threat we face from terrorism and serious and organised crime is global. It is inevitable that there will be circumstances where our security and intelligence agencies uncover threats to other countries through intelligence derived from a bulk interception warrant.

In some circumstances, such threats will be against countries with which the United Kingdom has well-established intelligence-sharing relationships, and in such circumstances there are likely to be corresponding safeguards applying to the handling of intercepted material. However, there will be occasions when such intelligence indicates a serious threat to a country overseas, potentially in urgent circumstances, whose authorities simply do not apply the same level of safeguards as those included in the Bill. In such circumstances, it is crucial that the Bill places a duty on the Secretary of State to consider the arrangements that should be in place to regulate the disclosure. This decision will need to balance the risk that the material will not be subject to the same level of safeguards that it would be in this country against the risks to the security of the country in question if material is not shared.

For example, in some circumstances a failure to share intercepted material containing vital intelligence could result in a terrorist atrocity. Even in such a scenario, the amendment would place an absolute prohibition on the relevant intercepted material being shared because the overseas authority does not apply safeguards corresponding to those in the Bill. This would not be a responsible position and I believe it is only right that the Secretary of State must be responsible for deciding the appropriate arrangements for sharing intercepted material with an overseas authority, considering the particular circumstances of each case. In addition to this consideration by the Secretary of State, the safeguards that apply to the use of bulk interception will be subject to rigorous, independent oversight and scrutiny by the Investigatory Powers Commissioner. This will, of course, include the arrangements for the disclosure of intercepted material overseas.

For the reasons I have outlined, it is absolutely crucial that the Bill provides for the Secretary of State to consider the extent to which corresponding safeguards should apply where intercepted material is being shared overseas. The amendment would fetter that consideration and is both unnecessary and potentially dangerous. Accordingly, I invite the noble Baroness not to move it.

Amendment 180 agreed.

Amendment 181

Moved by ***Earl Howe***

181: After Clause 137, insert the following new Clause—

"Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a bulk interception warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 137, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 137, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification."

Amendment 181 agreed.

Clause 138: Approval of major modifications made in urgent cases

Amendments 182 and 183

Moved by ***Earl Howe***

182: Clause 138, page 111, line 6, leave out "fifth" and insert "third"

183: Clause 138, page 111, line 15, at end insert—

"and section (Approval of major modifications by Judicial Commissioners)(4) does not apply in relation to the refusal to approve the decision."

Amendments 182 and 183 agreed.

Clause 141: Safeguards relating to retention and disclosure of material

Amendment 184

Moved by ***Earl Howe***

184: Clause 141, page 113, line 41, after "(5)" insert "and section 143"

Amendment 184 agreed.

Clause 142: Safeguards relating to disclosure of material overseas

Amendment 185

Moved by ***Earl Howe***

185: Clause 142, page 114, line 21, after "(5)" insert "and section 143"

Amendment 185 agreed.

Amendment 185A not moved.

Clause 144: Additional safeguards for items subject to legal privilege

Amendment 186

Moved by ***Earl Howe***

186: Clause 144, page 116, line 26, at end insert—

"( ) In deciding whether to give an approval under subsection (2) in a case where subsection (1)(b)(i) applies, a senior official must have regard to the public interest in the confidentiality of items subject to legal privilege."

Amendment 186 agreed.

Amendment 187

Moved by ***Earl Howe***

187: Clause 144, page 116, line 34, at end insert—

"( ) For the purposes of subsection (3)(b), there cannot be exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria unless—

(a) the public interest in obtaining the information that would be obtained by the selection of the intercepted content for examination outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury."

Amendment 188 (to Amendment 187) not moved.

Amendment 187 agreed.

Amendments 189 and 190

Moved by ***Earl Howe***

189: Clause 144, page 116, line 34, at end insert—

"(3A) Subsection (3B) applies if, in a case where intercepted content obtained under a bulk interception warrant is to be selected for examination—

(a) the selection of the intercepted content for examination meets any of the selection conditions in section 143(3)(a) to (c),

(b) the purpose, or one of the purposes, of using the criteria to be used for the selection of the intercepted content for examination ("the relevant criteria") is to identify communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to legal privilege, and

(c) the person to whom the warrant is addressed considers that the communications ("the targeted communications") are likely to be communications made with the intention of furthering a criminal purpose.

(3B) The intercepted content may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(3C) A senior official may give an approval under subsection (3B) only if the official considers that the targeted communications are likely to be communications made with the intention of furthering a criminal purpose."

190: Clause 144, page 116, line 36, after "examination," insert "for purposes other than the destruction of the item,"

Amendments 189 and 190 agreed.

Amendment 191

Moved by ***Earl Howe***

191: Clause 144, page 116, line 40, at end insert—

"(4A) The Investigatory Powers Commissioner may—

(a) direct that the item is destroyed, or

(b) impose conditions as to the disclosure or otherwise making available of that item.

(4B) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (4A), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(4C) Each of the following is an "affected party" for the purposes of subsection (4B)—

(a) the Secretary of State;

(b) the person to whom the warrant is or was addressed."

Amendments 192 and 193 (to Amendment 191) not moved.

Amendment 191 agreed.

Amendment 194

Moved by ***Earl Howe***

194: After Clause 144, insert the following new Clause—

"Additional safeguard for confidential journalistic material

Where—

(a) a communication which has been intercepted in accordance with a bulk interception warrant is retained, following its examination, for purposes other than the destruction of the communication, and

(b) it is a communication containing confidential journalistic material,

the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(For provision about the grounds for retaining material obtained under a warrant, see section 141.)"

Amendment 194 agreed.

Amendment 195

Moved by ***Lord Janvrin***

195: After Clause 144, insert the following new Clause—

"Offence of breaching safeguards relating to examination of material under bulk interception warrants

(1) A person commits an offence if—

(a) the person selects for examination any intercepted content or secondary data obtained under a bulk interception warrant,

(b) the person knows or believes that the selection of that intercepted content or secondary data for examination does not comply with a requirement imposed by section 143 or 144, and

(c) the person deliberately selects that intercepted content or secondary data for examination in breach of that requirement.

(2) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(3) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland."

Amendment 195 agreed.

Clause 146: Chapter 1: interpretation

Amendment 196

Moved by ***Earl Howe***

196: Clause 146, page 117, line 21, at end insert—

"section (General definitions: "journalistic material" etc.) (general definitions: "journalistic material" etc.),"

Amendment 196 agreed.

Clause 147: Power to issue bulk acquisition warrants

Amendment 196A

Moved by ***Lord Paddick***

196A: Clause 147, page 118, line 48, at end insert—

"( ) A bulk acquisition warrant may not require data which relates to or includes internet connection records."

Lord Paddick (LD): My Lords, Amendment 196A is in my name and that of my noble friend Lady Hamwee. It seeks to remove internet connection records from the type of communications data that can be acquired in bulk. Noble Lords will be very well aware of my views, and the agreed view of the Liberal Democrats, on internet connection records. We believe that they are unnecessary and disproportionate, for the reasons that I have articulated in detail throughout the passage of the Bill.

I shall just remind your Lordships what internet connection records mean. Internet service providers are being forced to keep a record of every website that everyone in the UK has visited in the last 12 months, whether the subscriber is suspected of crime or not. Even though only the first page of each website visited is shown, visiting www.relate.org.uk could, for example, immediately indicate that your marriage was in trouble. However there are some safeguards, including some concessions extracted by the Labour Opposition, to ensure that only the internet connection records of those suspected of crimes that could result on conviction in a sentence of 12 months' imprisonment or more can be examined by law enforcement agencies.

We are also grateful to the Labour Opposition for securing the review of bulk powers carried out by David Anderson QC, the Independent Reviewer of Terrorism Legislation. We are particularly grateful to David Anderson for highlighting in paragraph 2.41(b), on page 33 of his report on bulk powers, that,

"it is not currently envisaged that the bulk acquisition power in the Bill will be used to obtain internet connection records".

However, in a footnote at the bottom of that page, Mr Anderson states that he has been told,

"that this is no more than a statement of present practice and intention: neither the Bill nor the draft Code of Practice rules out the future use of the bulk acquisition power in relation to ICRs".

In Committee, the noble and learned Lord, Lord Keen, said:

"I can confirm to the Committee that the agencies do not currently acquire internet connection records in bulk and have no current intention to do so. It is however important to ensure that we do not legislate against the possibility of internet connection records being acquired in bulk, should agencies make a case which demonstrates that this might be necessary and proportionate in the interests of national security in future".—[*Official Report*, 7/9/16; cols. 1087-88.]

Surely we should be legislating for a proven need, not not legislating against a possible but unlikely proven one.

Noble Lords will remember that the security services—GCHQ, MI5 and MI6—have all said that they do not need internet connection records in order to do their work. The power to acquire communications data in bulk, including the power to acquire ICRs in bulk, is available only to those agencies. The power to acquire internet connection records in bulk is therefore not needed. They are not collected in bulk at the moment, and there is no current intention to do so. If this were an opposition amendment to include ICRs in bulk data acquisition, the Government would quite rightly say it was unnecessary. The power to acquire ICRs in bulk also strips away all the safeguards that are in place when law enforcement agencies apply for individual internet connection records.

This is the online equivalent of Section 44 of the Terrorism Act, which allowed the police to stop and search people without any reasonable suspicion. The former Home Secretary, now the Prime Minister, Theresa May took that power away from the police because she considered it disproportionate.

Lord Harris of Haringey (Lab): Surely Section 44 was for target hardening and deterrence rather than for any other purpose.

Lord Paddick: I am very grateful to the noble Lord, Lord Harris, but that is not what I understood Parliament's intention was when the legislation was enacted. We can argue the point. If the analogy with stop and

[LORD PADDICK]
search sounds familiar to noble Lords next to me, including the noble Lord, Lord Harris of Haringey, it is because it is an analogy that was used by the shadow Home Secretary Diane Abbott in describing the powers under the Bill, which she describes as draconian.

The pieces of this legislative jigsaw are beginning to fall into place. Telephone operators already keep a record of the details of every phone call made and every text message sent. Internet service providers are being forced by this Bill to keep a record of every website, you, I and everyone else in this country have visited over the previous 12 months, which is a provision this House agreed to on Monday in a Division when it rejected the Liberal Democrat amendment to prevent it. A request filter, operated by or on behalf of the Government will be constructed. It will have direct feeds into the databases of communications providers, including access to the sensitive personal information of every subscriber to telephone and internet services in the UK, every call they make and every website they visit. The House agreed to that provision in a Division on Monday when it rejected the Liberal Democrat amendment to prevent it. The power is then given by this part of the Bill to allow all that sensitive personal information—details of every phone call made and every website visited—to be downloaded at will by the security agencies with no further authorisation. I hope that at least some noble Lords are feeling uncomfortable at that prospect. Our amendment removes internet connection records from the data that can be acquired under a bulk acquisition warrant. I beg to move.

4.15 pm

Lord Carlile of Berriew (LD): My Lords, it will not surprise my noble friend to learn that I oppose the amendment that he has just moved. We made reference during our previous day on Report to papers that were presented by the Government at the time of First Reading. Those papers included, as was mentioned on Monday of this week, a paper in which GCHQ explained why the bulk acquisition of communications data material might be crucial to interdicting a major terrorism event which it thought was likely to occur, or might possibly occur, in the near future.

The issue was then referred to David Anderson—and I am surprised that my noble friend does not accept what Mr Anderson, the independent reviewer, said on the matter. He reminded us that three of the powers under review—bulk interception, bulk acquisition of communications data and bulk personal datasets—were already in use across the range of MI5, MI6 and GCHQ activity, from cyberdefence, counterterrorism and counterespionage to combating child sexual abuse and organised crime. He said:

"They play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield".

The GCHQ paper to which I referred dealt with "further afield".

Mr Anderson continued:

"After close examination of numerous case studies, the review concluded that other techniques could sometimes, though not always, be used to achieve these objectives: but that they would often be less effective, more dangerous, more resource-intensive, more intrusive or slower".

Mr Anderson concluded that there was a proven operational case for three of the powers already in use, and he agreed that there was a distinct though as yet unproven operational case for the fourth power: bulk equipment interference. He also recognised the "breath-taking"—that was his word—pace of change in this area, and that we needed to make sure that the authorities had the proportionate powers that were required to protect this country, and other countries, from terrorism.

Therefore, the Bill provides the powers with a very elaborate set of protections. We also have—it is available in the Public Bill Office—the *Bulk Acquisition DRAFT Code of Practice*, dated autumn 2016: it is very recent. In paragraphs 3.10 and 3.11 of the code—and, indeed, elsewhere in the code—the most elaborate protections are described. For example, paragraph 3.10 contains operational guidance and advice for those who are dealing with these matters and states in terms:

"No interference with privacy should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means".

Paragraph 3.11 of the code sets out in four very carefully drafted bullet points the elements of proportionality that should be considered before the powers are used. It includes assessing whether other methods have been considered and whether those other methods could have provided a reasonable outcome without the necessity of the invasion of privacy which undoubtedly the provisions describe.

I therefore ask my noble friend to state, when he comes to reply to this short debate, what his view is of the code of practice—and, in particular, of the part to which I referred.

Lord Paddick: The amendment relates specifically to internet connection records being acquired, and I have yet to hear my noble friend address any of his remarks to the issue of those records.

Lord Carlile of Berriew: If my noble friend wants me to be specific, I will, but I was trying not to take up too much time. Let us take the example of a piece of information, given to a security service, that people in possession of a bulk delivery of a certain type of telecommunications equipment, say a phone brand, are involved in the planning of a terrorist event. In order to find out quickly who these people are, the authorities would need to attack the bulk, so as to exclude all people who are not involved in the planned event. This is an absolutely routine technique that is used. I see one or two of my noble friends turning round in surprise. If they are surprised, they have not even read modern spy novels, let alone about the reality of what is being done by intelligence agencies all around the world.

The answer to my noble friend is as simple as that. I will just repeat my question, because I would like him to reply to it in due course. I take it that he has read the code of practice. What is missing from the code of practice that is required in order to provide the protection he wishes for? It is all in the code of practice; it is all in the statute. I apologise for repeating something I said

on Monday, but these provisions, as drafted, are a careful and responsible response by a Government who wish to do no more than the state absolutely has to, safely, to protect their citizens.

Lord Rooker (Lab): I will answer that point. The Bill of course is not draconian in any way whatever. It is a modest response to the technology that exists today, and an attempt to look at the technology of tomorrow that we do not know about. That is part of the problem. I regret that I was a bit late and missed the first 20 seconds of the noble Lord's introduction, so I may have this wrong, but he gave the impression that David Anderson supported his amendment. One only has to go to the report published in August, from which I want to put two sentences on the record. Paragraph 6.16 says:

"There is a clear value in the use of bulk powers to eliminate lines of enquiry, so that resources can be concentrated elsewhere and disruption to the public minimised".

I do not think we should fetter the security services by this amendment. The other sentence from the report that I want to put on the record is in paragraph 6.47, at point (d):

"Even where alternatives might be available, they are frequently more intrusive than the use of bulk acquisition".

Most of the bulk acquisition will never, ever be read. The vast majority—99.999%—will never be read or studied by anybody, and it gives a false impression when the noble Lord says that all our telephone calls, internet searches, and web browsing will be read by someone. That is simply not true. What is more, he has been briefed and knows that that is the case. I do not see why the opponents of the Bill, in this House or the other House, should try to give a false impression of what it is trying to do. I hope the noble Lord tests the opinion of the House, because I would like it clearly on the record that he probably has little or no support for his amendment.

Lord Campbell of Pittenweem (LD): I can be brief. I must begin of course by expressing my regret that I do not agree with my noble friend on the Front Bench. There is nothing more insulting than the expression, "If you could only see what passes across my desk, you would take a different view". I do not use that expression, but I have to admit that I cannot expunge from my memory my experience as a member of the Intelligence and Security Committee and my contact during that period with the security services. Essentially, we are talking about a question of judgment. My judgment is legitimately assisted by the conclusions of the report from Mr David Anderson, who was, a bit like Moses, dispatched up the mountain and told to come back with tablets of stone. In particular he came back with case studies, and I defy anyone to read them and not be persuaded beyond all doubt of the necessity for the powers that we are discussing today. As my noble friend Lord Carlile has pointed out, Mr Anderson reached the proven conclusion of the operational purpose of three powers and made a further case in respect of the fourth.

Sometimes in the course of these deliberations we confine ourselves to the question of terrorism. As has been mentioned, I think in passing, we should always remember that these are powers that are apt to deal with the question of organised crime and, more particularly, in the rather febrile atmosphere that surrounds the matter, the question of child sexual abuse.

Mr Anderson made the observation, which I doubt anyone would wish to challenge, that the pace of technological change is frightening. We all carry a mobile phone in our pockets; if we think of the first one we ever got some 20 years ago and compare it with the capacity of the one that we now have, that is as powerful an illustration of technological change as one could imagine.

I suppose the question may arise as to whether what we are discussing is necessary and proportionate. I respectfully suggest that the nature of the threat—I noticed as soon as I came into the building that the threat level is still severe—and the experience across the Channel, plus the experience of the security services in dealing with plots, argues beyond peradventure that what is proposed here is both necessary and proportionate. For these reasons, I regret I will not be able to follow my noble friend Lord Paddick when he tests the opinion of the House.

Lord Oates (LD): My Lords, I support my noble friend Lord Paddick and the amendment that he has moved. I should say at the outset that I do not doubt for one moment the very severe threats that we face, nor the essential and dedicated work done by our security services and the police. In the coalition Government we had to tackle many of these issues, and the then Deputy Prime Minister was always as impatient with those who were careless about our security as he was with those who were careless about our liberty.

So I understand the reality of the threats that we face. However, I am afraid I cannot agree with my two noble friends who have just spoken. We have to be very clear what we are talking about in the amendment, which is specifically about ICRs. I think that in some of this debate we might have missed that point.

My noble friend Lord Carlile referred to the fact that powers were already in use, but the bulk powers in relation to ICRs obviously cannot be in place because the powers of the Bill granting the requirement to collect ICRs have not come into effect, so they are not collected in that way. I am surprised that my noble friend takes the view that he does, because during the whole course of the debate on the Bill he has made much of the point that he has been consistent. I am not clear why his position has changed so significantly on the collection of ICRs. As I have noted in our previous debates on the subject, on 25 May 2013, writing in the *Daily Mail*, my noble friend wrote the following:

"I, Lord Reid, Lord West and others of like mind have never favoured the recording of every website visited by every … user, though we have been accused of that".

Lord Carlile of Berriew: My noble friend is playing with language. I have never favoured the recording of every website use we make, and I do not support the recording of them now. It is the availability of the metadata that is important. I ask my noble friend to deal with the example I gave in answer to my noble friend Lord Paddick and tell us whether he thinks it is reasonable.

4.30 pm

Lord Oates: I am dealing with the fact that we are granting a power under the Bill, as this House voted only a couple of days ago, for all the websites visited by every user in this country, whether suspected of anything or innocent, to be recorded. That is a matter of fact, not a matter of debate.

We also need to deal with the canard that we have heard from people such as the noble Lord who spoke from the Labour Benches earlier, which is that to question the powers granted under the Bill is somehow to question the integrity of the police or the security and intelligence agencies, to cast aspersions on them. That is nonsense. I have nothing but respect for the difficult, often dangerous and always demanding jobs carried out on our behalf by the police and security services. There is no doubt that the vast majority of them do so with absolute dedication and integrity, but it is absurd to suggest that such powers are not on occasion abused. We know they are. That is a matter of fact; it is recorded in our history. Of course, it is inevitable that that is the case: all such agencies are made up of human beings and we are all subject to frailty. That is why, over the years, those who believe in constitutional democracy have insisted on limiting the powers granted to the state and its agents.

That is why we have such concern about the power granted after our debate the other day to record—I repeat—every website visited by every person in this country. The Government will now have the power to demand that that be recorded. That is why we are concerned about that and about the bulk power in relation to it. That is why I will be supporting my noble friend Lord Paddick and my colleagues on the Front Bench: I think that is rightly a matter of grave concern for liberties in this country.

Lord King of Bridgwater (Con): My Lords, I think the noble Lord accepts one thing: the use of these powers, which are very substantial, could in certain circumstances be essential to obstruct or prevent an otherwise very serious terrorist incident. I am not sure whether he challenges that. The noble Lord, Lord Carlile, referred to the supporting evidence from David Anderson to that effect. So the noble Lord, Lord Oates, is taking the courageous position—as is the noble Lord, Lord Paddick—of being prepared to accept that risk. In the current situation, nobody in this House has any right to be ignorant that the threat at present is severe—and "severe" may be slightly underplaying the scale of the situation at the moment. We know the situation; there is no point drawing attention to it. We know what is happening in Mosul at present, where the instruction among ISIS is, "Don't hang around here. Get into some of the capitals of the West and see what you can do". The message is going out to try to cause a terrorist incident right on our doorstep.

Lord Oates: The noble Lord asks me specifically what I believe. It is very simple. I do not believe that we should record the websites visited by every person in this country. I do not think that is merited; it is not a power used by any other "Five Eyes" country or any constitutional democracy that I know of.

Lord King of Bridgwater: So the noble Lord does not agree with David Anderson or with those who said that this could be an essential asset and ingredient in possibly preventing a serious terrorist attack. He is saying that he does not believe that that is true, if I understand him; if he believes that it is true, he is being extremely courageous, in the words of "Yes Minister", in taking that position. He is taking responsibility for what might happen to people in this country, which is a very brave thing to do.

I do not want to interfere with the slight divisions of view that are appearing among the Liberal Democrats in this House, but I have listened to the noble Lord, Lord Paddick, in a number of these debates. He is very conscientious and he looks as though he has worked very hard in preparing his brief and making speeches in support of the amendments, but he only ever gives us about half the story. He suggested in earlier debates that we were looking for powers that the agencies have not asked for and did not want, and said that he did not know why they were in the Bill. He knows the police—it is the police who are keen to get those powers. He did not put that in his speech; he did not tell the House the background, or that this was not some quirk of the noble Earl, Lord Howe, who wanted to shove stuff into the Bill for his own amusement. That is where that came from. I was disappointed by the noble Lord's presentation of the amendment, as was exposed by the noble Lord, Lord Carlile. I do not think I heard a single mention of David Anderson or his report in the presentation of this amendment, although I may be wrong.

What stands out in this whole debate is that the Government know that these are very substantial powers, which nobody would wish to see if we could avoid it—and they are there because of the serious threat we face. The Government have recognised that if you are to have those powers, they must be surrounded by the most substantial safeguards there can be. I am known to be a critic of how much time the Government took before the Bill came forward. A number of us thought that there was an urgency about the matter and tried to get it earlier. But the Government have gone to great lengths, setting out the Anderson report and now, as the noble Lord, Lord Carlile, said, producing the code of practice. There was not a single mention from the noble Lord, Lord Paddick, of the code of practice, and I do not know whether he has considered it. I should like him to answer the question of the noble Lord, Lord Carlile. What does he think of the code of practice? It is a further safeguard that the Government have included in these proposals.

We have to protect our citizens. A number of us live with the threat of terrorism in our lives, in one way or another, and we know the tragedies it can cause in so many different fields. Sometimes we have to take tough and regrettable steps to make sure that innocent people—that everybody—is protected as far as possible. If that happens, I am determined to see that we do it in a situation and structure in which every possible protection is included against abuse and every possible system of accountability for their exercise is kept up to date and regularly inspected. The very elaborate provision that the Government have made in this Bill generally commands respect, except in one or two quarters,

where people are still fighting an old battle about what old rights should be and how there should be no interference. In the modern situation in which we live, we must have proper provision to protect our nation and, at the same time, ensure that there is every possible safeguard against abuse.

The Lord Bishop of Chester: My Lords, I am sure we do not want to prolong this debate. As I said on Monday, I was a member of the pre-legislative scrutiny group. You might wonder why a Bishop was invited to be part of that exercise, but I think it was because of this point—the ethics of interference with privacy. I am sorry that the discussion so far has almost become too polarised, because the noble Lord, Lord Paddick, is making a serious point, which I demonstrate by quoting David Anderson in his evidence to the Joint Committee on Human Rights. He said:

"I think there is a human rights issue in relation to this Bill that dwarfs all the others, and it is the question of the compatibility of bulk collection and retention of data with Article 8 of the European convention".

The noble Lords, Lord Paddick and Lord Oates, make a serious point and we should acknowledge it, even if we come down on the side of the noble Lord, Lord King—as I do—that these powers are necessary and proportionate. The argument is about the safeguards—namely, that the warrant has to be personally signed by the Secretary of State, lapses after six months if it is not renewed, and is subject to the judicial commissioners. The real argument is about that. I do not think internet connection records are in principle different from other things that might be intercepted. However, I acknowledge the serious ethical point that the noble Lords, Lord Paddick and Lord Oates, raised, even if I come down on the side of the Government and the noble Lord, Lord King, in opposing the amendment.

Baroness Harding of Winscombe (Con): My Lords, I fear that we are repeating the debate we had the day before yesterday. If noble Lords look at this amendment, they will see three reasons why they could support it. One is if they feel that bulk data powers are unacceptable in any circumstances. A second is if they feel that the elaborate controls referred to by my noble friend Lord King and the noble Lord, Lord Carlile, are not good enough. The third is if they object in principle to the collection of internet connection records. From what I have heard this afternoon, the argument of the noble Lord, Lord Paddick, is entirely the third point. I respect his view on internet connection records but we debated this on Monday and the view of the House was very clear. I fear that we are simply repeating that discussion. We should move on.

Lord Rosser (Lab): As the noble Lord, Lord Paddick, said, David Anderson QC commented in his report that neither the Bill nor the draft code of practice rules out the future use of the bulk acquisition power for internet connection records. Internet connection records are not currently acquired in bulk but existing legislation already permits the agencies to acquire such records in bulk, albeit there appears to be no present intention to do so.

The effect of this amendment would be to remove an existing legislative provision which could be needed in the future for bulk acquisition—bulk acquisition which David Anderson QC found had contributed significantly to the disruption of terrorist operations and, through that disruption, almost certainly to the saving of lives, and which had also been demonstrated to be crucial in a variety of fields. In addition, any such application in the future to obtain such data by the security and intelligence agencies would be covered by the relevant safeguards in the Bill, including in relation to necessity and proportionality in the interests of national security and the approval process.

This Bill is, among other things, about the appropriate balance between security and privacy. We clearly have a different view from that of some other noble Lords on where that appropriate balance lies. Our view is that, for the reasons I have sought to set out, we are unable to support this amendment and, if it is put to a vote, we shall oppose it.

Lord Keen of Elie: My Lords, this amendment would remove the ability for the intelligence agencies to acquire internet connection records in bulk, an issue we have already discussed in Committee and revisited on a number of occasions, as observed by my noble friend Lady Harding. At the time we debated this in Committee, I highlighted the point now made by the noble Lord, Lord Rosser, that this is not a new power introduced by the Bill. This is an existing power. It exists in legislation, albeit, while it is provided for, it is not at present utilised.

As I explained in Committee, it is vital in the current climate, when methods of electronic communication are changing and developing at an exponential rate, that we provide technology-neutral legislation—a point made by the noble Lord, Lord Rooker. We remain of the view that we would not wish to legislate against the possibility of internet connection records being acquired in bulk, should the agencies make a case—and they must make a case—which demonstrates that this might be necessary and proportionate in the interests of national security.

We strongly believe that it is right that the intelligence agencies have the power to acquire communications data in bulk, and David Anderson supported this in his bulk powers review. The noble Lords, Lord Carlile and Lord Campbell of Pittenweem, alluded to the observations made by David Anderson. I will refer to only one further quotation: he said that,

"bulk acquisition has contributed significantly to the disruption of terrorist operations and, though that disruption, almost certainly the saving of lives".

The noble Lord, Lord Carlile, alluded to some of the examples that were given by David Anderson and worked through in his report.

4.45 pm

Any application to obtain communications data in bulk—including, should it be necessary, internet connection records—will be subject to the strong safeguards the Bill introduces, which have been discussed at length during the Bill's scrutiny. A warrant to acquire communications data in bulk must be both necessary on one of the grounds set out in the Bill, one of which

[Lord Keen of Elie]
must be national security, and proportionate to what is sought to be achieved. It must specify the operational purposes for which the data can be selected for examination, and of course will be subject to the double lock of Secretary of State and judicial commissioner approval. In addition, as the noble Lord, Lord Carlile, pointed out, there are the further provisions and ring-fencing provided for in the bulk acquisition code of practice.

In the context of these very strong safeguards we consider it right that, as currently, the bulk acquisition power should remain technologically neutral, with the safeguards applying equally to all types of communications data defined by the Bill. The most fundamental safeguard is that any request to acquire internet connection records in bulk would need to be judged necessary and proportionate by both the Secretary of State and a judicial commissioner. That is a powerful safeguard, and on that basis I invite the noble Lord to withdraw the amendment.

Lord Paddick: I am grateful to the Minister and to other noble Lords who have contributed to this debate. As regards the comments of my noble friend Lord Carlile of Berriew, despite my request that he specifically address the issue of internet connection records, I did not hear him do so. We are not against the bulk acquisition of communications data in general or per se. We oppose only the bulk acquisition of internet connection records as part of those data.

On the question my noble friend Lord Carlile raised about the codes of practice, of course they are comprehensive. However, through this amendment we are trying to prevent internet connection records being acquired in bulk, which is allowed for in the codes of practice.

The noble Lord, Lord Rooker, was of a different opinion from the one that I quoted—that the Bill was draconian. I am grateful to him for giving me the opportunity to emphasise to the House that it was the current Labour shadow Home Secretary, Diane Abbott, who described the Bill as draconian.

Lord Rooker: For the avoidance of doubt, I understood that—that was the point I made.

Lord Paddick: I did not suggest in any way that David Anderson agreed with this amendment, or that the lists of everybody's websites would be read, as the noble Lord, Lord Rooker, suggested.

As regards the comments made by my noble friend Lord Campbell of Pittenweem, he referred to case studies in the David Anderson report on bulk data. I cannot emphasise this enough to noble Lords: internet connection records do not currently exist. The telecommunications companies will have to create them. Therefore any case studies in David Anderson's report do not relate to the bulk collection of internet connection records. Internet connection records do not exist, so they cannot be collected in bulk at the moment.

I acknowledge the great experience of the noble Lord, Lord King of Bridgwater, and his passion about these issues. He emphasised that everything needs to be done to prevent a terrorist attack, and I agree with him 100%. The point that I made in my opening speech when I quoted David Anderson directly, saying that it was a direct quote from him, was that GCHQ, MI5 and MI6—the agencies responsible for keeping us safe from terrorism—say that they do not need internet connection records. Even the Minister said that at present there is no anticipated need to collect internet connection records to prevent a terrorist attack.

I am very grateful to the right reverend Prelate the Bishop of Chester for saying that we are making a fundamental point here. The difference between today's debate and Monday's debate is that requiring individuals' internet connection records has to be based on reasonable suspicion. Thanks to the intervention of the Labour Front Bench, the level of the seriousness of the crime that needs to be suspected before those records can be handed over is higher than the Government first suggested. However, this power would allow everybody's internet connection records to be acquired in bulk by the security agencies with no reasonable suspicion at all.

Lord King of Bridgwater: Will the noble Lord—

Lord Paddick: I am sorry but this is Report and I do not have to give way, unless the noble Lord wishes to clarify what I have just said.

Lord King of Bridgwater: I wish to make an intervention. The noble Lord said again that nobody wants this power. Can he explain why it is in the Bill?

Lord Paddick: It is not for me to explain why the Government want in the Bill a power that currently does not exist, because internet connection records do not exist, and which the security services say they do not want but which the noble and learned Lord says might be needed in the future. It is not for me to justify this power; I am saying to the House why I do not believe it is justified. The noble and learned Lord and the noble Lord, Lord Rosser, made the point that this is an existing power, but how can you have an existing power to acquire something that will not exist until the Bill is enacted?

I have tried to explain very clearly—although unfortunately some people have not heard what I have said—why we cannot accept this provision, and that is why I want to test the opinion of the House.

4.52 pm

Division on Amendment 196A

Contents 82; Not-Contents 321.

Amendment 196A disagreed.

Division No. 1

CONTENTS

Addington, L.	Bowles of Berkhamsted, B.
Alderdice, L.	Bradshaw, L.
Bakewell of Hardington Mandeville, B. [Teller]	Bruce of Bennachie, L.
Barker, B.	Burt of Solihull, B.
Beith, L.	Chidgey, L.
Benjamin, B.	Clancarty, E.
Bonham-Carter of Yarnbury, B.	Dholakia, L.
	Doocey, B.
	Erroll, E.

Foster of Bath, L.
Fox, L.
Garden of Frognal, B.
Glasgow, E.
Goddard of Stockport, L.
Greaves, L.
Grender, B.
Hamwee, B.
Harris of Richmond, B.
Humphreys, B. [Teller]
Hussain, L.
Hussein-Ece, B.
Janke, B.
Jolly, B.
Jones of Cheltenham, L.
Kennedy of The Shaws, B.
Kirkwood of Kirkhope, L.
Kramer, B.
Loomba, L.
Low of Dalston, L.
Ludford, B.
Mackenzie of Framwellgate, L.
Maclennan of Rogart, L.
McNally, L.
Marks of Henley-on-Thames, L.
Miller of Chilthorne Domer, B.
Newby, L.
Northover, B.
Oates, L.
Oxford and Asquith, E.
Paddick, L.
Pinnock, B.
Purvis of Tweed, L.
Randerson, B.
Razzall, L.
Redesdale, L.
Rennard, L.
Roberts of Llandudno, L.
Rodgers of Quarry Bank, L.
Scott of Needham Market, B.
Sharkey, L.
Sheehan, B.
Shipley, L.
Shutt of Greetland, L.
Smith of Newnham, B.
Stephen, L.
Stoneham of Droxford, L.
Storey, L.
Strasburger, L.
Stunell, L.
Suttie, B.
Taverne, L.
Taylor of Goss Moor, L.
Thomas of Gresford, L.
Thomas of Winchester, B.
Thornhill, B.
Thurso, V.
Tonge, B.
Tope, L.
Tyler, L.
Tyler of Enfield, B.
Wallace of Saltaire, L.
Walmsley, B.
Wigley, L.
Wood of Anfield, L.
Wrigglesworth, L.

NOT CONTENTS

Adams of Craigielea, B.
Ahmad of Wimbledon, L.
Ahmed, L.
Alli, L.
Anderson of Swansea, L.
Andrews, B.
Anelay of St Johns, B.
Arbuthnot of Edrom, L.
Armstrong of Hill Top, B.
Armstrong of Ilminster, L.
Arran, E.
Ashton of Hyde, L.
Astor, V.
Astor of Hever, L.
Attlee, E.
Baker of Dorking, L.
Bassam of Brighton, L.
Bates, L.
Beecham, L.
Berkeley of Knighton, L.
Bertin, B.
Bilimoria, L.
Billingham, B.
Black of Brentwood, L.
Blackstone, B.
Blencathra, L.
Bloomfield of Hinton Waldrist, B.
Borwick, L.
Bourne of Aberystwyth, L.
Bowness, L.
Brabazon of Tara, L.
Bridgeman, V.
Brooke of Alverthorpe, L.
Brookman, L.
Brougham and Vaux, L.
Brown of Eaton-under-Heywood, L.
Browne of Belmont, L.
Browning, B.
Buscombe, B.
Butler of Brockwell, L.
Byford, B.
Caithness, E.
Callanan, L.
Campbell of Pittenweem, L.
Campbell-Savours, L.
Carlile of Berriew, L.
Carrington of Fulham, L.
Cathcart, E.
Cavendish of Furness, L.
Chadlington, L.
Chalker of Wallasey, B.
Chester, Bp.
Chisholm of Owlpen, B.
Clark of Windermere, L.
Clarke of Hampstead, L.
Collins of Highbury, L.
Colville of Culross, V.
Colwyn, L.
Cooper of Windrush, L.
Cope of Berkeley, L.
Cork and Orrery, E.
Cormack, L.
Corston, B.
Courtown, E. [Teller]
Cox, B.
Craigavon, V.
Crickhowell, L.
Cromwell, L.
Davidson of Glen Clova, L.
Davies of Oldham, L.
Davies of Stamford, L.
De Mauley, L.
Dear, L.
Deech, B.
Denham, L.
Dixon-Smith, L.
Dobbs, L.
Donaghy, B.
Donoughue, L.
Drake, B.
Drayson, L.
D'Souza, B.
Dundee, E.
Dunlop, L.
Dykes, L.
Eaton, B.
Eccles, V.
Eccles of Moulton, B.
Elton, L.
Empey, L.
Evans of Bowes Park, B.
Evans of Watford, L.
Evans of Weardale, L.
Fairfax of Cameron, L.
Falkland, V.
Fall, B.
Farmer, L.
Faulkner of Worcester, L.
Faulks, L.
Fellowes, L.
Fink, L.
Finlay of Llandaff, B.
Finn, B.
Fookes, B.
Ford, B.
Forsyth of Drumlean, L.
Foulkes of Cumnock, L.
Framlingham, L.
Freeman, L.
Freud, L.
Gadhia, L.
Gale, B.
Gardiner of Kimble, L.
Gardner of Parkes, B.
Garel-Jones, L.
Geddes, L.
Gilbert of Panteg, L.
Glasman, L.
Glendonbrook, L.
Goldie, B.
Golding, B.
Goodlad, L.
Gordon of Strathblane, L.
Goudie, B.
Grade of Yarmouth, L.
Grantchester, L.
Greengross, B.
Greenway, L.
Griffiths of Burry Port, L.
Grocott, L.
Hailsham, V.
Hameed, L.
Hamilton of Epsom, L.
Hanham, B.
Harding of Winscombe, B.
Harries of Pentregarth, L.
Harris of Haringey, L.
Haskel, L.
Hastings of Scarisbrick, L.
Haworth, L.
Hayman, B.
Hayter of Kentish Town, B.
Hayward, L.
Healy of Primrose Hill, B.
Helic, B.
Henig, B.
Henley, L.
Higgins, L.
Hodgson of Abinger, B.
Hodgson of Astley Abbotts, L.
Hogg, B.
Hollick, L.
Hollis of Heigham, B.
Holmes of Richmond, L.
Hooper, B.
Horam, L.
Howard of Lympne, L.
Howard of Rising, L.
Howarth of Newport, L.
Howe, E.
Howe of Idlicote, B.
Howell of Guildford, L.
Howells of St Davids, B.
Hughes of Woodside, L.
Hunt of Wirral, L.
Hutton of Furness, L.
Inglewood, L.
Irvine of Lairg, L.
James of Blackheath, L.
Janvrin, L.
Jenkin of Kennington, B.
Jones, L.
Jones of Whitchurch, B.
Jopling, L.
Judd, L.
Keen of Elie, L.
Kennedy of Southwark, L.
Kerr of Kinlochard, L.
Kilclooney, L.
King of Bridgwater, L.
Kirkham, L.
Kirkhill, L.
Kirkhope of Harrogate, L.
Lamont of Lerwick, L.
Lang of Monkton, L.
Lawrence of Clarendon, B.
Lawson of Blaby, L.
Lea of Crondall, L.
Lee of Trafford, L.
Leigh of Hurley, L.
Lennie, L.
Liddell of Coatdyke, B.
Liddle, L.
Lindsay, E.
Lingfield, L.
Lipsey, L.
Listowel, E.
Liverpool, E.
Lothian, M.
Lucas, L.
Luce, L.
Lyell, L.
McAvoy, L.
McColl of Dulwich, L.
MacGregor of Pulham Market, L.
McGregor-Smith, B.
McInnes of Kilwinning, L.
McIntosh of Hudnall, B.
McIntosh of Pickering, B.
Mackay of Clashfern, L.
McKenzie of Luton, L.
Magan of Castletown, L.
Manzoor, B.
Marland, L.
Marlesford, L.
Maxton, L.
Mendelsohn, L.
Mobarik, B.
Monks, L.
Montrose, D.
Morgan of Huyton, B.
Morris of Bolton, B.
Morris of Handsworth, L.
Morris of Yardley, B.
Moynihan, L.
Murphy of Torfaen, L.
Naseby, L.
Nash, L.
Neville-Jones, B.
Neville-Rolfe, B.
Nicholson of Winterbourne, B.

Noakes, B.
Norton of Louth, L.
Nye, B.
O'Cathain, B.
O'Neill of Clackmannan, L.
Oppenheim-Barnes, B.
O'Shaughnessy, L.
Pannick, L.
Patel of Bradford, L.
Pendry, L.
Pidding, B.
Pitkeathley, B.
Popat, L.
Porter of Spalding, L.
Prescott, L.
Prosser, B.
Quin, B.
Ramsay of Cartvale, B.
Rana, L.
Rawlings, B.
Redfern, B.
Ridley, V.
Robathan, L.
Rogan, L.
Rooker, L.
Rose of Monewden, L.
Rosser, L.
Rowe-Beddoe, L.
Royall of Blaisdon, B.
Ryder of Wensum, L.
Sassoon, L.
Scott of Bybrook, B.
Seccombe, B.
Selborne, E.
Selkirk of Douglas, L.
Selsdon, L.
Sheikh, L.
Sherbourne of Didsbury, L.
Shields, B.
Shinkwin, L.
Simon, V.
Skelmersdale, L.
Smith of Basildon, B.
Smith of Hindhead, L.
Somerset, D.
Spicer, L.
Stedman-Scott, B.
Sterling of Plaistow, L.
Stoddart of Swindon, L.
Stone of Blackheath, L.
Stowell of Beeston, B.
Stroud, B.
Sugg, B.
Suri, L.
Sutherland of Houndwood, L.
Symons of Vernham Dean, B.
Taylor of Blackburn, L.
Taylor of Holbeach, L. [Teller]
Temple-Morris, L.
Thomas of Swynnerton, L.
Tomlinson, L.
Touhig, L.
Trees, L.
Trefgarne, L.
Trimble, L.
True, L.
Tugendhat, L.
Tunnicliffe, L.
Uddin, B.
Ullswater, V.
Vere of Norbiton, B.
Verma, B.
Vinson, L.
Wasserman, L.
Watkins of Tavistock, B.
Watson of Invergowrie, L.
Watts, L.
Wei, L.
Wheatcroft, B.
Wheeler, B.
Whitaker, B.
Willetts, L.
Williams of Trafford, B.
Wills, L.
Wilson of Tillyorn, L.
Woolf, L.
Young of Cookham, L.
Young of Norwood Green, L.
Young of Old Scone, B.
Younger of Leckie, V.

5.07 pm

Clause 153: Modification of warrants

Amendments 197 and 198

Moved by ***Earl Howe***

197: Clause 153, page 122, line 17, leave out subsection (6)

198: After Clause 153, insert the following new Clause—

"Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a bulk acquisition warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 153, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 153, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification."

Amendments 197 and 198 agreed.

Clause 154: Approval of major modifications made in urgent cases

Amendments 199 and 200

Moved by ***Earl Howe***

199: Clause 154, page 123, line 15, leave out "fifth" and insert "third"

200: Clause 154, page 123, line 24, at end insert—

"and section (Approval of major modifications by Judicial Commissioners)(4) does not apply in relation to the refusal to approve the decision."

Amendments 199 and 200 agreed.

Clause 159: Safeguards relating to the retention and disclosure of data

Amendments 201 and 202

Moved by ***Earl Howe***

201: Clause 159, page 127, line 10, after "(5)" insert "and section 160"

202: Clause 159, page 127, line 18, after "(5)" insert "and section 160"

Amendments 201 and 202 agreed.

Amendment 203

Moved by ***Lord Butler of Brockwell***

203: After Clause 160, insert the following new Clause—

"Offence of breaching safeguards relating to examination of data

(1) A person commits an offence if—

(a) the person selects for examination any communications data obtained under a bulk acquisition warrant,

(b) the person knows or believes that the selection of that data for examination does not comply with a requirement imposed by section 160, and

(c) the person deliberately selects that data for examination in breach of that requirement.

(2) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(3) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland."

Amendment 203 agreed.

Clause 163: Bulk equipment interference warrants: general

Amendment 203A

Moved by ***Lord Paddick***

203A: Clause 163, leave out Clause 163

Lord Paddick: My Lords, the amendment is in my name and that of my noble friend Lady Hamwee. I shall speak also to all the other amendments in this group, Amendments 203B to 203D, 204A to 204F, 205A, 208A to 208C, 209A, 210A and 210B, 215A, 217A and 218A. The sole effect of all the amendments would be to remove from the Bill the power to engage in bulk equipment interference.

This is a new power for the security and intelligence agencies to carry out equipment interference in bulk overseas. It is not a power they currently have and, according to David Anderson QC, it is not something that they currently do. As a result, David Anderson said in his review of bulk powers that the operational case for bulk equipment interference was "not yet proven". The noble Lord, Lord Murphy, has said:

"The case for bulk equipment interference was less strong, but nevertheless still there".—[*Official Report*, 7/9/2016; col. 1049.]

As the noble Lord, Lord Rosser, said in Committee, there is a difference between an operational case, let alone an unproven one, and proportionality or desirability. Quoting Mr Anderson, he pointed out that Mr Anderson assessed only the operational cases in his review, saying that the issues of proportionality and necessity were a matter for Parliament—which is why we are debating these amendments today.

We heard in earlier debates about the potentially broad scope of targeted equipment interference warrants. They can specify all equipment used by anyone in a particular organisation or more than one organisation involved in a single investigation or operation; all equipment used by members of a group with a common purpose or engaged in a particular activity; equipment in a particular location or more than one location for the purpose of a single investigation or operation; and equipment being used or that may be used for a particular activity or activities. That is all contained in Clause 108.

Although I realise that the primary focus of this House should be to protect the citizens of this country, I ask noble Lords to consider how they would feel if overseas Governments took our lead and enacted similar legislation that could be deployed against the UK and its citizens. UK citizens' communications could be acquired through the use of bulk equipment interference warrants if they communicated with others based overseas.

In paragraph 7.37 of his report into bulk powers, David Anderson QC warns that considerable caution is required for a series of reasons. He concludes in paragraph 7.38:

"All this means that bulk EI will require, to an even greater extent than the other powers subject to review, the most rigorous scrutiny not only by the Secretary of State but by the Judicial Commissioners who must approve its use and by the IPC which will have oversight of its consequences".

It is the nearest David Anderson comes to expressing an opinion on necessity and proportionality and, reading between the lines, it is clear that he is not keen.

For those reasons—and as the Intelligence and Security Committee initially recommended, although it was subsequently persuaded—we believe that bulk equipment interference warrants should be removed from the Bill. I beg to move.

The Minister of State, Ministry of Defence (Earl Howe) (Con): My Lords, these amendments would remove the bulk equipment interference provisions from the Bill. Before I address the amendments specifically, it is worth pausing to reflect briefly on the importance of bulk powers in the round and the very significant steps that the Government have taken to ensure both that a robust operational case has been made for their necessity and that the most rigorous safeguards will apply to their use.

Extremely detailed and extensive scrutiny has been applied to bulk powers during the passage of the Bill, both in Parliament and, of course, by David Anderson QC as part of his bulk powers review. The conclusion of that review was that bulk powers,

"have a clear operational purpose";

that they,

"play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield";

and that where alternatives exist to their use,

"they were likely to produce less comprehensive intelligence and were often more dangerous (for example to agents and their handlers), more resource-intensive, more intrusive or—crucially—slower".

The Government have now tabled amendments giving full effect to the sole recommendation of that review, establishing in statute a Technology Advisory Panel to the Investigatory Powers Commissioner. We have also accepted an amendment tabled by the Intelligence and Security Committee which introduces a specific offence in the Bill to address deliberate misuse of the bulk powers. We have addressed wider concerns of that committee by adding very significant detail to the Bill on the safeguards that will regulate the use of these powers. I am grateful for the intensive scrutiny that has been applied to the bulk provisions in the Bill and believe that those provisions are all the stronger for it. There should now be no question that these powers are necessary and they are subject to world-leading safeguards.

5.15 pm

I now turn to the specific amendments tabled by the Liberal Democrats. Bulk equipment interference is, as the noble Lord, Lord Paddick, said, a foreign-based

[Earl Howe]
power. It comprises a set of techniques to obtain information from devices in order to identify threats to the UK's national security in circumstances where the vital intelligence is not available through the use of other methods. Material acquired under a bulk equipment interference warrant will be subject to enhanced access controls once it has been collected, ensuring that only relevant material is selected for examination and providing strong privacy protections. Equipment interference is not new. The security and intelligence agencies already use this power to keep us safe. Bulk equipment interference could be authorised under existing legislation—the Intelligence Services Act 1994—but without the strong statutory safeguards that we are providing in the Bill.

Targeted equipment interference powers are already used at scale to identify threats overseas, alongside other powers such as bulk interception, but terrorists, criminals and hostile states continue to embrace new technology to evade detection. As a result, the security and intelligence agencies face an increasingly partial and fragmented intelligence picture, even when investigating known threats. If the security and intelligence agencies are to maintain their ability to identify and disrupt threats, they will need to use other, complementary techniques. Bulk equipment interference is one such technique and in some cases may be the only way that vital intelligence can be collected. The Bill puts that power on a new statutory footing, increasing transparency and strengthening safeguards.

Bulk equipment interference has been the subject of thorough scrutiny throughout the passage of the Bill. To inform that scrutiny, the Government have published an unprecedented amount of information on the power. This has included factsheets, a draft code of practice, an operational case for all the bulk powers and the findings of the review of bulk powers undertaken by David Anderson QC. The Intelligence and Security Committee of Parliament, which has studied this power in great detail, has been clear that the bulk equipment interference regime is entirely necessary. As the chair of the committee, my right honourable and learned friend Dominic Grieve MP said at Second Reading in the other place:

"Following publication of our report, we received additional evidence from the agencies as to why they need bulk equipment interference warrants to remain in the Bill and they actually made a persuasive case. More importantly, the Committee was reassured that information obtained by such means will be treated in exactly the same way, with exactly the same controls, as data acquired under a bulk interception warrant. The Committee is therefore broadly content that there is a valid case for the power to remain in the Bill".—[*Official Report*, Commons, 15/3/16; col. 838]

Nevertheless, in order to provide further information to Parliament the Government agreed to a review of the operational case for bulk powers by David Anderson QC, the Independent Reviewer of Terrorism Legislation. His findings make clear why bulk equipment interference is so crucial. The noble Lord, Lord Paddick, has not quoted him, I suggest, in a balanced way. In his report David Anderson found that,

"an operational case for bulk EI has been made out in principle",

and went on to state that,

"there are likely to be real-world instances in which no effective alternative is available".

The security and intelligence agencies have been unequivocal that bulk equipment interference will be absolutely essential to protect the nation from those who mean to do us harm. Removing the power from the Bill would impede this. Clearly, that is not something that David Anderson's report condones or recommends; nor is it a recommendation of the Intelligence and Security Committee or of the other place, both of which have also given thorough consideration to this power. That is why the Government are legislating for this power, which will become only more vital as terrorists and criminals continue to take advantage of the internet and associated technology.

However, the noble Lord, Lord Paddick, was correct in one statement that he made: David Anderson's report did go on to recommend that "rigorous scrutiny" is applied to the use of bulk equipment interference by the Secretary of State, judicial commissioners and the Investigatory Powers Commissioner. The Bill and its associated draft code of practice require rigorous consideration of the benefits and risks of any operation and robust oversight of the use of the power more generally. To complement those provisions, a new Technology Advisory Panel will be established, which will ensure that the Investigatory Powers Commissioner will always be aware of the changes in technology that impact on the use of the bulk powers.

I believe that bulk equipment interference is truly a vital power, and the Bill serves only to ensure that its use is subject to strict and transparent safeguards. There is no reason or recommendation to prohibit the security and intelligence agencies from using this power. I therefore invite the noble Lord to withdraw his amendment.

Lord Paddick: I am grateful to the Minister for his comments. He kept saying that this power to conduct bulk equipment interference was absolutely essential to keeping us safe. What I do not understand is, first, why the very broad powers provided and the very broad range of targets that could be specified using targeted equipment interference could not be used in almost every case, rather than this power. Secondly, if bulk equipment interference is absolutely essential, if it could be authorised under existing legislation, why has it never been used by the security services? That is what David Anderson says.

As the Minister took the opportunity to talk about bulk powers in the round, perhaps I might get two things on the record. First, I cannot stress strongly enough that we are not opposed to the bulk acquisition of communications data generally. We are not opposed to bulk powers generally. We have specific issues with specific powers. Secondly, it has been suggested to me that I am standing here saying these things because it is my party policy. My party policy was decided by a working group that I chaired. I wrote the conclusions to that policy paper. I not only agree with the conclusions of that policy paper, I believe that they are absolutely the right conclusions. However, we have made the points that we wanted to make. They are on the record. I beg leave to withdraw the amendment.

Amendment 203A withdrawn.

Clause 164: Meaning of "equipment data"

Amendment 203B not moved.

Clause 165: Power to issue bulk equipment interference warrants

Amendment 203C not moved.

Clause 166: Approval of warrants by Judicial Commissioners

Amendment 203D not moved.

Clause 167: Approval of warrants issued in urgent cases

Amendment 204

Moved by ***Earl Howe***

204: Clause 167, page 132, line 37, leave out "(unless already cancelled) ceases to have effect" and insert "—

(a) ceases to have effect (unless already cancelled), and

(b) may not be renewed;

and section 166(4) does not apply in relation to the refusal to approve the decision."

Amendment 204 agreed.

Amendment 204A not moved.

Clause 168: Failure to approve warrant issued in urgent case

Amendment 204B not moved.

Clause 169: Decisions to issue warrants to be taken personally by Secretary of State

Amendment 204C not moved.

Clause 170: Requirements that must be met by warrants

Amendment 204D not moved.

Clause 171: Duration of warrants

Amendment 204E not moved.

Clause 172: Renewal of warrants

Amendment 204F not moved.

Clause 173: Modification of warrants

Amendment 205

Moved by ***Earl Howe***

205: Clause 173, page 137, line 10, leave out subsection (7)

Amendment 205 agreed.

Amendment 205A not moved.

Amendment 206

Moved by ***Earl Howe***

206: After Clause 173, insert the following new Clause—

"Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a bulk equipment interference warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary, and

(b) in the case of a major modification adding or varying any description of conduct authorised by the warrant, whether the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matters referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 173, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 173, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification."

Amendment 206 agreed.

Clause 174: Approval of major modifications made in urgent cases

Amendments 207 and 208

Moved by ***Earl Howe***

207: Clause 174, page 138, line 13, leave out "fifth" and insert "third"

208: Clause 174, page 138, line 22, at end insert—

"and section (Approval of major modifications by Judicial Commissioners)(4) does not apply in relation to the refusal to approve the decision."

Amendments 207 and 208 agreed.

Amendment 208A not moved.

Clause 175: Cancellation of warrants

Amendment 208B not moved.

Clause 176: Implementation of warrants

Amendment 208C not moved.

Clause 177: Safeguards relating to retention and disclosure of material

Amendment 209

Moved by ***Earl Howe***

209: Clause 177, page 141, line 4, after "(5)" insert "and section 179"

Amendment 209 agreed.

Amendment 209A not moved.

Clause 178: Safeguards relating to disclosure of material overseas

Amendment 210

Moved by ***Earl Howe***

210: Clause 178, page 141, line 28, after "(5)" insert "and section 179"

Amendment 210 agreed.

Amendment 210A not moved.

Clause 179: Safeguards relating to examination of material etc.

Amendment 210B not moved.

Clause 180: Additional safeguards for items subject to legal privilege

Amendments 211 to 215

Moved by ***Earl Howe***

211: Clause 180, page 143, line 29, at end insert—

"( ) In deciding whether to give an approval under subsection (2) in a case where subsection (1)(b)(i) applies, a senior official must have regard to the public interest in the confidentiality of items subject to legal privilege."

212: Clause 180, page 143, line 37, at end insert—

"( ) For the purposes of subsection (3)(b), there cannot be exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria unless—

(a) the public interest in obtaining the information that would be obtained by the selection of the material for examination outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury."

213: Clause 180, page 143, line 37, at end insert—

"(3A) Subsection (3B) applies if, in a case where protected material obtained under a bulk equipment interference warrant is to be selected for examination—

(a) the selection of the material for examination meets any of the selection conditions in section 179(3)(a) to (c),

(b) the purpose, or one of the purposes, of using the criteria to be used for the selection of the material for examination ("the relevant criteria") is to identify communications or other items of information that, if they were not communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose, would be items subject to legal privilege, and

(c) the person to whom the warrant is addressed considers that the communications or other items of information ("the targeted communications or other items of information") are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose.

(3B) The material may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(3C) A senior official may give an approval under subsection (3B) only if the official considers that the targeted communications or other items of information are likely to be communications made or (as the case may be) other items of information created or held with the intention of furthering a criminal purpose."

214: Clause 180, page 143, line 38, after "retained" insert ", for purposes other than the destruction of the item,"

215: Clause 180, page 143, line 43, at end insert—

"(4A) The Investigatory Powers Commissioner may—

(a) direct that the item is destroyed, or

(b) impose conditions as to the disclosure or otherwise making available of that item.

(4B) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (4A), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(4C) Each of the following is an "affected party" for the purposes of subsection (4B)—

(a) the Secretary of State;

(b) the person to whom the warrant is or was addressed."

Amendments 211 to 215 agreed.

Amendment 215A not moved.

Amendment 216

Moved by ***Earl Howe***

216: After Clause 180, insert the following new Clause—

"Additional safeguard for confidential journalistic material

Where—

(a) material obtained under a bulk equipment interference warrant is retained, following its examination, for purposes other than the destruction of the material, and

(b) it is material containing confidential journalistic material,

the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(For provision about the grounds for retaining material obtained under a bulk equipment interference warrant, see section 177.)"

Amendment 216 agreed.

Amendment 217

Moved by ***Lord Butler of Brockwell***

217: After Clause 180, insert the following new Clause—

"Offence of breaching safeguards relating to examination of material

(1) A person commits an offence if—

(a) the person selects for examination any material obtained under a bulk equipment interference warrant,

(b) the person knows or believes that the selection of that material does not comply with a requirement imposed by section 179 or 180, and

(c) the person deliberately selects that material in breach of that requirement.

(2) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(3) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland."

Amendment 217 agreed.

Clause 181: Application of other restrictions in relation to warrants

Amendment 217A not moved.

Clause 182: Chapter 3: interpretation

Amendment 218

Moved by ***Earl Howe***

218: Clause 182, page 144, line 28, at end insert—

"section (General definitions: "journalistic material" etc.) (general definitions: "journalistic material" etc.),"

Amendment 218 agreed.

Amendment 218A not moved.

Clause 186: Restriction on use of class BPD warrants

Amendment 219

Moved by ***Lord Keen of Elie***

219: Clause 186, page 145, line 36, at end insert—

"(A1) An intelligence service may not retain, or retain and examine, a bulk personal dataset in reliance on a class BPD warrant if the head of the intelligence service considers that the bulk personal dataset consists of, or includes, protected data.

For the meaning of "protected data", see section (Meaning of "protected data")."

Lord Keen of Elie: My Lords, this group contains a number of amendments specific to Part 7 of the Bill, which covers bulk personal datasets. I first turn to government Amendments 219, 220, 224, 226, 227, 229, 230, 237, 238, 239, 240 and 265, 266 and 267.

In David Anderson QC's review of bulk powers he stated:

"It has come to my attention that some",

bulk personal datasets,

"may contain material that is comparable to the content of communications, and in rare cases even material subject to",

legal professional privilege. He continued:

"In the light of these facts I have already recommended to the Home Office that consideration be given to the introduction of additional safeguards to the Bill and Code of Practice".

We welcome David Anderson's review and the attention he has given to these matters. I stress that it is unlikely to be the case that many bulk personal datasets will contain this sort of material, but in those instances where they do, it is right that it is protected appropriately. These amendments ensure that the Bill provides such protection.

Amendment 219 explains that an intelligence agency may not use a class BPD warrant to,

"retain, or retain and examine, a bulk personal dataset",

that consists of or includes "protected data". Amendment 220 would insert a new clause which defines what protected data are in this context. In essence, protected data are the same class of data as "content" in the telecommunications context or "protected material" in the equipment interference context. Protected data in a bulk personal dataset may include, for example, the contents of letters, emails or other documents. They do not include identifying data—for example, data that may help to identify persons, systems, services, locations or events—nor do they include systems data, which are data that enable or facilitate the functioning of any system or service.

5.30 pm

If the data cannot be classified as either identifying data or systems data, then they will fall within the definition of protected data so long as they are private information. Non-private information that would fall outside the definition may include publicly available information, such as books, newspapers, TV and radio broadcasts and data that are freely available online and are not subject to any privacy settings or access controls.

Amendment 227 is a new clause which gives the Secretary of State the power to impose conditions which must be satisfied before protected data may be selected for examination where an individual is known to be in the British Islands at the time of selection. The bulk personal datasets code of practice will provide further detail on what those conditions will be. The draft code of practice published by the Government before Report includes an annex of indicative text that the Government propose including in the body of the code if Parliament passes these amendments.

I now turn to government Amendments 239 and 240. These two new clauses outline additional safeguards for items subject to legal professional privilege in bulk personal datasets. As David Anderson noted, material

subject to legal professional privilege would only rarely be contained in a bulk personal data set, but again the Government agree that in those instances where datasets contain this sort of material, it is right that it is protected appropriately.

Amendment 239 is a new clause which outlines additional safeguards which apply when protected data subject to legal professional privilege are selected for examination. These safeguards will apply where the purpose of selecting protected data for examination is to identify any items subject to legal privilege or if it is likely to identify such items. Amendment 240 provides additional safeguards for the retention of items subject to legal professional privilege following examination. These amendments give effect to David Anderson's recommendations and ensure that legally privileged protected data retained in reliance on a specific bulk personal dataset warrant are subject to the same stringent safeguards that apply when data are examined under Part 6.

Amendments 224, 226, 229, 230, 237, 238, 265, 266 and 267 are consequential amendments to the amendments I have outlined.

Government Amendments 221, 222, 223 and 225 specify the information that must be included about operational purposes in class and specific BPD warrant applications. These are technical drafting amendments that bring the drafting of Part 7 into line with the drafting of Part 6.

Amendments 235 and 242 are technical amendments to make clear the test that a judicial commissioner should apply when reviewing two particular decisions made under Part 7. That test is the same one that is applied throughout the Bill. Although this is clear in many places in the Bill, there is currently no explicit language on this point in Clauses 200 and 203. These are essentially tidying-up amendments to rectify this point.

Finally in this group I turn to government Amendment 236. This is a minor and technical amendment to ensure consistency of drafting with equivalent provisions in Part 6. In short, it ensures that particular requirements on the Secretary of State relating to the safeguards for the examination of material by the agencies are the same for Part 7 as they are for Part 6.

Taken together the amendments in this group add further safeguards to and otherwise fine-tune the provisions in Part 7. I beg to move.

Amendment 219 agreed.

Amendment 220

Moved by ***Lord Keen of Elie***

220: After Clause 186, insert the following new Clause—

"Meaning of "protected data"

(1) In this Part, "protected data" means any data contained in a bulk personal dataset other than data which is one or more of the following—

(a) systems data;

(b) data which falls within subsection (2);

(c) data which is not private information.

(2) The data falling within this subsection is identifying data which—

(a) is contained in the bulk personal dataset,

(b) is capable of being logically separated from the bulk personal dataset, and

(c) if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of any of the data which would remain in the bulk personal dataset or of the bulk personal dataset itself, disregarding any meaning arising from the existence of that data or (as the case may be) the existence of the bulk personal dataset or from any data relating to that fact.

(3) For the meaning of "systems data" see section 239(4).

(4) In this section, "private information" includes information relating to a person's private or family life."

Amendment 220 agreed.

Clause 187: Class BPD warrants

Amendment 221

Moved by ***Lord Keen of Elie***

221: Clause 187, page 146, line 21, leave out from "service" to end of line 23 and insert "is seeking authorisation for the examination of bulk personal datasets of that class, the operational purposes which it is proposing should be specified in the warrant (see section 194)"

Amendment 221 agreed.

Clause 188: Specific BPD warrants

Amendments 222 to 226

Moved by ***Lord Keen of Elie***

222: Clause 188, page 147, line 13, leave out "wishes" and insert "is seeking authorisation"

223: Clause 188, page 147, line 18, leave out "wishes" and insert "is seeking authorisation"

224: Clause 188, page 147, line 22, leave out "186(1)" and insert "186(A1), (1)"

225: Clause 188, page 147, line 30, leave out from "service" to end of line 32 and insert "is seeking authorisation for the examination of the bulk personal dataset, the operational purposes which it is proposing should be specified in the warrant (see section 194)"

226: Clause 188, page 147, line 34, leave out "186(1)" and insert "186(A1), (1)"

Amendments 222 to 226 agreed.

Amendment 227

Moved by ***Lord Keen of Elie***

227: After Clause 189, insert the following new Clause—

"Protected data: power to impose conditions

Where the Secretary of State decides to issue a specific BPD warrant, the Secretary of State may impose conditions which must be satisfied before protected data retained in reliance on the warrant may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection."

Amendment 227 agreed.

Clause 191: Approval of specific BPD warrants issued in urgent cases

Amendment 228

Moved by ***Earl Howe:***

228: Clause 191, page 150, line 19, at end insert—

"and section 190(4) does not apply in relation to the refusal to approve the decision."

Amendment 228 agreed.

Clause 194: Requirements that must be met by warrants

Amendment 229

Moved by ***Earl Howe:***

229: Clause 194, page 152, line 9, at end insert ", and

(d) where the Secretary of State has imposed conditions under section (Protected data: power to impose conditions), specify those conditions."

Amendment 229 agreed.

Clause 196: Renewal of warrants

Amendment 230

Moved by ***Earl Howe:***

230: Clause 196, page 154, line 3, at end insert—

"( ) Section (Protected data: power to impose conditions) applies in relation to the renewal of a specific BPD warrant as it applies in relation to the issue of such a warrant (whether or not any conditions have previously been imposed in relation to the warrant under that section)."

Amendment 230 agreed.

Clause 197: Modification of warrants

Amendment 231

Moved by ***Earl Howe:***

231: Clause 197, page 154, line 37, leave out subsection (6)

Amendment 231 agreed.

Amendment 232

Moved by ***Earl Howe:***

232: After Clause 197, insert the following new Clause—

"Approval of major modifications by Judicial Commissioners

(1) In deciding whether to approve a decision to make a major modification of a class BPD warrant or a specific BPD warrant, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the modification is necessary on any of the grounds on which the Secretary of State considers the warrant to be necessary.

(2) In doing so, the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter referred to in subsection (1) with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(3) Where a Judicial Commissioner refuses to approve a decision to make a major modification under section 197, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to make a major modification under section 197, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to make the modification."

Amendment 232 agreed.

Clause 198: Approval of major modifications made in urgent cases

Amendments 233 and 234

Moved by ***Earl Howe:***

233: Clause 198, page 155, line 33, leave out "fifth" and insert "third"

234: Clause 198, page 155, line 42, at end insert—

"and section (Approval of major modifications by Judicial Commissioners)(4) does not apply in relation to the refusal to approve the decision."

Amendments 233 and 234 agreed.

Clause 200: Non-renewal or cancellation of BPD warrants

Amendment 235

Moved by ***Earl Howe:***

235: Clause 200, page 157, line 7, at end insert—

"( ) In deciding whether to give approval for the purposes of subsection (3)(b), the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy)."

Amendment 235 agreed.

Clause 202: Safeguards relating to examination of bulk personal datasets

Amendments 236 to 238

Moved by ***Earl Howe:***

236: Clause 202, page 159, line 9, after "that" insert "arrangements are in force for securing that"

237: Clause 202, page 159, line 18, at end insert—

"( ) The Secretary of State must also ensure, in relation to every specific BPD warrant which specifies conditions imposed under section (Protected data: power to impose conditions), that arrangements are in force for securing that any selection for examination of protected data on the basis of criteria which are referable to an individual known to be in the British Islands at the time of the selection is in accordance with the conditions specified in the warrant."

238: Clause 202, page 159, line 19, leave out "subsection (2)" and insert "this section"

Amendments 236 to 238 agreed.

Amendments 239 and 240

Moved by ***Earl Howe:***

239: After Clause 202, insert the following new Clause—

"Additional safeguards for items subject to legal privilege: examination

(1) Subsections (2) and (3) apply if, in a case where protected data retained in reliance on a specific BPD warrant is to be selected for examination—

(a) the purpose, or one of the purposes, of using the criteria to be used for the selection of the data for examination ("the relevant criteria") is to identify any items subject to legal privilege, or

(b) the use of the relevant criteria is likely to identify such items.

(2) If the relevant criteria are referable to an individual known to be in the British Islands at the time of the selection, the data may be selected for examination using the relevant criteria only if the Secretary of State has approved the use of those criteria.

(3) In any other case, the data may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(4) The Secretary of State may give approval for the purposes of subsection (2) only with the approval of a Judicial Commissioner.

(5) Approval may be given under subsection (2) or (3) only if—

(a) the Secretary of State or (as the case may be) the senior official considers that the arrangements mentioned in section 188(6)(d) include specific arrangements in respect of items subject to legal privilege, and

(b) where subsection (1)(a) applies, the Secretary of State or (as the case may be) the senior official considers that there are exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria.

(6) In deciding whether to give an approval under subsection (2) or (3) in a case where subsection (1)(a) applies, the Secretary of State or (as the case may be) the senior official must have regard to the public interest in the confidentiality of items subject to legal privilege.

(7) For the purposes of subsection (5)(b), there cannot be exceptional and compelling circumstances that make it necessary to authorise the use of the relevant criteria unless—

(a) the public interest in obtaining the information that would be obtained by the selection of the data for examination outweighs the public interest in the confidentiality of items subject to legal privilege,

(b) there are no other means by which the information may reasonably be obtained, and

(c) obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury.

(8) In deciding whether to give approval for the purposes of subsection (4), the Judicial Commissioner must—

(a) apply the same principles as would be applied by a court on an application for judicial review, and

(b) consider the matter with a sufficient degree of care as to ensure that the Judicial Commissioner complies with the duties imposed by section 2 (general duties in relation to privacy).

(9) Subsections (10) and (11) apply if, in a case where protected data retained in reliance on a specific BPD warrant is to be selected for examination—

(a) the purpose, or one of the purposes, of using the criteria to be used for the selection of the data for examination ("the relevant criteria") is to identify data that, if the data or any underlying material were not created or held with the intention of furthering a criminal purpose, would be an item subject to legal privilege, and

(b) the person to whom the warrant is addressed considers that the data ("the targeted data") or any underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose.

(10) If the relevant criteria are referable to an individual known to be in the British Islands at the time of the selection, the data may be selected for examination using the relevant criteria only if the Secretary of State has approved the use of those criteria.

(11) In any other case, the data may be selected for examination using the relevant criteria only if a senior official acting on behalf of the Secretary of State has approved the use of those criteria.

(12) Approval may be given under subsection (10) or (11) only if the Secretary of State or (as the case may be) the senior official considers that the targeted data or the underlying material is likely to be data or underlying material created or held with the intention of furthering a criminal purpose.

(13) In this section, "underlying material", in relation to data retained in reliance on a specific BPD warrant, means any communications or other items of information from which the data was produced."

240: After Clause 202, insert the following new Clause—

"Additional safeguards for items subject to legal privilege: retention following examination

(1) Where an item subject to legal privilege is retained following its examination in reliance on a specific BPD warrant, for purposes other than the destruction of the item, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as is reasonably practicable.

(2) The Investigatory Powers Commissioner may—

(a) direct that the item is destroyed, or

(b) impose conditions as to the disclosure or otherwise making available of that item.

(3) The Investigatory Powers Commissioner—

(a) may require an affected party to make representations about how the Commissioner should exercise any function under subsection (2), and

(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(4) Each of the following is an "affected party" for the purposes of subsection (3)—

(a) the Secretary of State;

(b) the person to whom the warrant is or was addressed."

Amendments 239 and 240 agreed.

Amendment 241

Moved by ***Lord Janvrin***

241: After Clause 202, insert the following new Clause—

"Offence of breaching safeguards relating to examination of material

(1) A person commits an offence if—

(a) the person selects for examination any data contained in a bulk personal dataset retained in reliance on a class BPD warrant or a specific BPD warrant,

(b) the person knows or believes that the selection of that data is in breach of a requirement specified in subsection (2), and

(c) the person deliberately selects that data in breach of that requirement.

(2) The requirements specified in this subsection are that any selection for examination of the data—

(a) is carried out only for the specified purposes (see subsection (3)),

(b) is necessary and proportionate, and

(c) if the data is protected data, satisfies any conditions imposed under section (Protected data: power to impose conditions).

(3) The selection for examination of the data is carried out only for the specified purposes if the data is selected for examination only so far as is necessary for the operational purposes specified in the warrant in accordance with section 194.

In this subsection, "specified in the warrant" means specified in the warrant at the time of the selection of the data for examination.

(4) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(5) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland."

Amendment 241 agreed.

Clause 203: Application of Part to bulk personal datasets obtained under this Act

Amendment 242

Moved by ***Earl Howe:***

242: Clause 203, page 160, line 11, at end insert—

"( ) In deciding whether to give approval for the purposes of subsection (7), the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review."

Amendment 242 agreed.

Schedule 8: Combination of warrants and authorisations

Amendment 243

Moved by ***Lord Keen of Elie***

243: Schedule 8, page 242, line 7, at end insert—

"( ) In sub-paragraph (1) "enactment" does not include any primary legislation passed or made after the end of the Session in which this Act is passed."

Lord Keen of Elie: My Lords, I will now address government amendments relating to definitions and extent, and consequential provisions. They aim to ensure consistency within the Bill and with other statutes. Clause 246 contains the usual power to make amendments to other legislation consequential on the provisions of the Bill. Schedule 8 contains a similar power to make amendments consequential on the provisions in that schedule. As currently drafted, the powers would permit the amendment of legislation passed at any time in future.

The power to make consequential amendments to future enactments is necessary because other Bills before Parliament at the same time as this Bill touch upon the powers and public authorities covered by the Bill—such as, for example, the Policing and Crime Bill. Since it is impossible to predict how those Bills, or the Investigatory Powers Bill, may be amended during their parliamentary passage, and which Bill may achieve Royal Assent first, it is necessary to allow for the possibility of consequential amendment of future enactments.

In its recent report on the powers in the Bill, the Delegated Powers and Regulatory Reform Committee recommended that the powers should be restricted to the amending of future enactments passed or made during the current Session. The Government indicated in Committee in this House that they intended to accept this recommendation. Amendments 243 and 281 give effect to the committee's recommendation, and I commend them to the House.

Amendments 260 and 271 are technical amendments that remove the definition of "person" from the Bill. The Bill's definition of "person" in Clause 239 was carried over from the Regulation of Investigatory Powers Act 2000. It does not apply in relation to Parts 2 or 5 of the Bill, and we have concluded that it is not needed in respect of the other parts. The Interpretation Act definition will apply throughout the Bill. The definition of "person" in Clause 239 is therefore not required and Amendments 260 and 271 simply remove it.

Amendment 268 provides definitions of "journalistic material" and "confidential journalistic material". It makes it clear where the additional protections provided for in Parts 2 and 5 of the Bill, which we debated here on the first day of Report, will apply. It is of course the case that the Government are seeking to protect legitimate journalism while ensuring that those who wish to do us harm cannot hide behind spurious claims of journalism. For this reason, Amendment 268 makes it clear that material acquired or created to further a criminal purpose is not considered journalistic material in the context of the Bill. This seeks to

[Lord Keen of Elie]
prevent persons such as those in the media wing of Daesh attracting a safeguard intended for legitimate journalists.

Amendments 280 and 286 clarify the drafting in relation to the definition of a postal operator, and to consequential amendments being made to RIPA. These drafting amendments make no changes to the effect of the provisions. Amendments 282, 283, 284 and 292 make minor amendments to the Security Service Act 1989, Intelligence Services Act 1994, Police Act 1997 and Anti-terrorism, Crime and Security Act 2001 in consequence of the updated targeted-interception provisions in Part 2 of this Bill.

Amendment 289 relates to the IPC's duties to report to Scottish Ministers. Where the Police Act 1997 requires the IPC to report certain matters to Scottish Ministers, this amendment provides that the IPC can do so at any time, as opposed to only in its annual report. Amendment 285 is a minor and consequential amendment. As we have discussed previously, the Bill provides for an interception warrant to be obtained that has the main purpose of obtaining secondary data from communications, rather than intercepting communications content. This amendment simply amends RIPA to make it clear that a notice served under Part 3 of that Act can relate to an interception warrant that has the main purpose only of obtaining secondary data.

Amendment 287 ensures that the provisions of RIPA will make proper reference to powers provided for in this Bill, alongside existing legislative references. It will make two key changes to RIPA. First, it inserts a reference in Section 48 of RIPA to the equipment interference powers provided for in the Bill, which will sit alongside existing references to property interference powers contained in the Intelligence Services Act 1994 and the Police Act 1997. This amendment makes it clear that references to surveillance in Part 2 of RIPA do not include equipment interference activity which will be authorised under the Bill when it becomes the Investigatory Powers Act. This minor amendment will simply ensure consistency with the existing drafting of RIPA.

Secondly, and similarly, the amendment inserts a reference to equipment interference warrants into Schedule 2 to RIPA, which will sit alongside an existing reference to property interference authorisations under Part 3 of the Police Act 1997. Schedule 2 to RIPA relates to the issuing of a Section 49 notice under Part 3 of RIPA. A Section 49 notice allows relevant authorities to require a person to put protected electronic information into an "intelligible form". In the future, acquisitions of these types of data will be done using equipment interference powers provided for in the Bill, so it is essential that law enforcement agencies continue to be able to use Section 49 notices with the new statutory framework. This amendment ensures that, in future, a law enforcement chief or an appropriate delegate will retain the same powers they currently hold in relation to protected electronic information obtained under existing legislation.

Amendment 288 is a minor, technical amendment that corrects a drafting error in Schedule 10. Paragraph 62 of Schedule 10 amends the Regulation of Investigatory Powers (Scotland) Act 2000 to ensure that Scottish Ministers can issue a code of practice in relation to equipment interference. This amendment clarifies that any such code of practice will be limited to targeted equipment interference so far as it relates to the police service or the Police Investigations and Review Commissioner, and will not relate to bulk equipment interference, a power which is not authorised by Scottish Ministers.

Finally, Amendments 296 to 300 are technical amendments which simply clarify the extent of the provisions of the Bill in relation to the Crown dependencies. They make two key changes. The first is being made following a request from the Isle of Man Government and will enable the extension of any of the provisions of the Bill, with or without modification, to the Isle of Man. This could assist the Isle of Man in ensuring that its legislative framework for law enforcement can be fully up to date and future-proof, enabling greater consistency with UK law.

The second of these changes will provide a more limited extension of provision for the Channel Islands, simply ensuring that any amendments made by the Bill to the provisions of another Act, such as the consequential amendments detailed at Schedule 10, may be extended to the Channel Islands by Order in Council, if that Act contains such a power. Any extension by Order in Council would of course only take place in consultation with the Governments of Jersey and Guernsey, and with their consent, and they would retain the option to make those amendments in domestic legislation instead. These technical amendments will help to clarify the extent of the provisions of the Bill. I beg to move.

5.45 pm

Lord Low of Dalston (CB): My Lords, I shall speak to Amendments 294 and 295, tabled by the noble Baronesses, Lady Hollins and Lady O'Neill, and the noble and learned Lords, Lord Falconer and Lord Wallace. The noble Baronesses very much regret that they cannot be present in the House today, and they have asked me to speak to their amendments. I will be brief, as I understand that, without prejudice to the Government's ultimate position, the Minister is not seeking to divide the House, and we are all most grateful to him for that.

The amendments would have no impact on the security measures in the Bill, nor would they affect the other measures in the Bill in any way. Their sole purpose is to bring into force automatically after Royal Assent Clause 8 and the new clause that was added to the Bill by this House last week by a large majority.

The amendments would deliver cost protections in hacking cases, which Section 40 of the Crime and Courts Act 2013 was enacted to provide for all publication torts. Section 40 is a key part of the Leveson recommendations that the Government promised to implement but has not been commenced. Non-commencement frustrates the will of Parliament and is a breach of the 2013 cross-party agreement. The commencement of these clauses automatically after Royal Assent is necessary to ensure that the device of

non-commencement is not employed again on the amendments that the House passed last week. For these reasons, I commend Amendments 294 and 295 to the House.

Lord Keen of Elie: My Lords, we discussed the substantive points on this issue on day one of Report. We consider these amendments consequential to the ones we discussed then. Although the Government's position on the substantive issue remains as we set out last week, we are not opposing these amendments.

Amendment 243 agreed.

Clause 225: Payments towards certain compliance costs

Amendment 244

Moved by ***Baroness Hamwee***

244: Clause 225, page 178, line 12, leave out from "receive" to end of line 14 and insert "their relevant costs"

Baroness Hamwee: My Lords, I shall also speak to Amendments 245 and 246. These amendments take us back to the question of the reimbursement of the operators' costs. We have heard frequent assurances about the operators' compliance costs and that they are to be met, but the words of the Bill do not quite live up to some of the narrative.

Our three amendments cover two alternatives; they would not all be possible. Amendments 244 and 245 would provide that arrangements were in force to secure for the operators the full amount of all relevant costs—"relevant costs" are defined later in the clause—not an appropriate contribution. As Clause 225(1) is framed, the Secretary of State must ensure,

"an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate".

With these two amendments, we seek to take out that element of discretion.

Amendment 246 would provide that if the contribution was not an equal amount, there should be regulations regarding the basis of how the contribution is calculated. Our amendments provide that the Secretary of State should lay regulations to that effect. It will be obvious to noble Lords that our reasons are transparency, equality between operators and the opportunity to consider the criteria—the factors, if you like—applied in calculating the contribution. In other words, our intention is scrutiny, using the opportunity that regulations give for debate of their content.

We have debated this matter on a number of occasions, and the Minister will be well aware of our concern. This is an attempt, at this almost last stage, to pin down just how the contribution will be made. I beg to move.

Earl Howe: My Lords, Amendments 244 and 245 are intended to ensure that communications service providers are fully reimbursed for their costs in connection with complying with obligations under the Bill. As the noble Baroness knows, this matter has been considered at length both in this House and in the Commons. It is important to recognise that service providers must not be unduly disadvantaged financially for complying with obligations placed on them aimed at protecting national security or combating crime. Indeed, the Government have a long history of working with service providers on these matters and we have been absolutely clear that we are committed to cost recovery.

I once again take the opportunity to reaffirm to the House a point that both my right honourable friend the former Security Minister and my right honourable friend the Prime Minister made very clear in the other place and that I made in Committee: this Government will reimburse 100% of reasonable costs incurred by communications service providers in relation to the acquisition and retention of communications data. This includes both capital and operational costs, including the costs associated with the retention of internet connection records.

The question that the House needs to consider, I submit, is whether it is appropriate for the Parliament of today to tie the hands of future Governments on this issue. That does not mean that we take our commitment lightly, or that future Governments will necessarily or lightly change course. Indeed, it is unlikely that any change in policy will ever take place. For example, the current policy has not changed since the passage of the Regulation of Investigatory Powers Act 2000, and so has survived Governments of three different colours, or combinations of colours.

The Bill adds further safeguards, requiring a data retention notice to set out the level of contribution that applies. This ensures that the provider must be consulted on any changes to the cost model and means that the provider could seek a review of any variation to the notice which affected the level of contribution.

Another question that I hope the House will consider is whether a communications service provider should be able to derive commercial benefit as a result of the obligations imposed on them in relation to the other powers under the Bill. Sometimes, it may be necessary for a communications service provider to upgrade part of its infrastructure to comply with an obligation imposed on it under a technical capability notice. As the communications service providers may be able to derive some business benefit from that upgrade, it is right that the legislation allows for the contribution to the costs to be appropriate to the circumstances.

Some noble Lords have expressed concern about the term "reasonable costs" and asked what it means. I hope I can provide some reassurance on that point. Significant public funding is made available to companies to ensure that they can provide assistance to public authorities in tackling terrorism, crime and other threats. As costs are reimbursed from public funds, the codes of practice make very clear that companies should take value for money into account when procuring, operating and maintaining the infrastructure required to comply with a notice. Were a company to select a solution that did not deliver best value for public funds, I am sure noble Lords would agree that it is absolutely right that the Government would need to consider carefully whether those costs were reasonable and therefore whether it was appropriate to reimburse the company in full.

[Earl Howe]

The noble Baroness's Amendment 246 acknowledges that there may be circumstances where it is appropriate for a communications service provider to be reimbursed less than its full costs. However, we do not think her proposed regulations provide the required flexibility. As I just explained, communications service providers may receive some business benefit from the changes made to their systems and it is appropriate that the Government are able to discuss these matters with them on a case-by-case basis, rather than be bound by general regulations. Indeed, while communications service providers would welcome an amendment to require 100% cost recovery in all cases, I suggest that they are unlikely to welcome regulations which enshrine in law circumstances where they would not receive full reimbursement.

I hope I have allayed any concerns about the Government's position on costs and accordingly invite the noble Baroness to withdraw her amendment.

Baroness Hamwee: My Lords, until the last two or three sentences, I thought the noble Earl had made a much better case for regulations than I did. I am a little worried about his argument that regulations cannot provide for flexibility. Flexibility is not necessarily bad, but how it is exercised should be transparent, and that is what my amendment is driving at.

The noble Earl started his remarks by saying that the operators should not be "unduly disadvantaged", and it is those words which caveat the commitment that has troubled us throughout our debates. We have tried, particularly with the third amendment, to meet the points made by the Government. I will obviously not pursue this any further; we have reached the end of the road. I have no doubt that someone will draw to our attention any problem in practice in future. I beg leave to withdraw the amendment.

Amendment 244 withdrawn.

Amendments 245 and 246 not moved.

Clause 228: National security notices

Amendment 247

Moved by ***Earl Howe***

247: Clause 228, page 180, line 18, at end insert—

"( ) In a case where—

(a) a national security notice would require the taking of any steps, and

(b) in the absence of such a notice requiring the taking of those steps, the taking of those steps would be lawful only if a warrant or authorisation under a relevant enactment had been obtained,

the notice may require the taking of those steps only if such a warrant or authorisation has been obtained."

Earl Howe: My Lords, I shall speak also to the other government amendments. Government Amendments 247 to 250 clarify the activity that can be authorised by a national security notice to provide greater reassurance to telecommunications operators to whom such a notice may be given. These amendments also respond to concerns raised in the Commons that the detail set out in the draft code of practice was clearer than the provisions in the Bill.

Clause 228 states that the Secretary of State may give such a notice to a telecommunications operator in the UK, requiring the taking of such specified steps as are considered necessary in the interests of national security. The type of support that may be required includes the provision of services or facilities which would help the intelligence agencies to safeguard the security of their personnel and operations, or provide assistance with an emergency as defined in Section 1 of the Civil Contingencies Act 2004.

Amendment 248 makes it clear that a national security notice cannot be used for the primary purpose of acquiring communications or data. The proposed amendments further clarify that, in any circumstance where the taking of a step set out in the notice would involve the acquisition of private data, any interference with privacy must be authorised by an appropriate warrant or other authorisation under the Bill, or another relevant statute, where it is available. Therefore, a notice, of itself, cannot authorise as its primary purpose an intrusion into an individual's privacy.

I should like to emphasise here that this power can be exercised only if the Secretary of State and a judicial commissioner are satisfied that the conduct required by a notice is necessary and proportionate to what is sought to be achieved.

In addition, Amendment 250 makes it clear that any conduct required under a notice is lawful for all purposes, providing reassurance for telecommunications operators that, when conduct is carried out in accordance with the requirements of a notice, the operator will not risk being found to be in breach of any other legal requirement.

I hope that these amendments reassure noble Lords that a national security notice cannot be used to circumvent the need to obtain a warrant or authorisation, but neither could it prohibit the acquisition of private data when such conduct has been appropriately authorised.

6 pm

Amendments 255 to 258 propose the inclusion of additional safeguards to the notice-giving regime in Part 9. The Government amended the Bill in the Commons to provide an explicit necessity and proportionality test before the Secretary of State may give a technical capability notice or national security notice, and made it clear that a notice cannot be given until a judicial commissioner approves the decision. I propose extending these important safeguards to Clause 232, which makes provision for the Secretary of State to vary or revoke a notice. Taken together, these amendments would ensure that the Secretary of State must consider the necessity and proportionality of any new obligations imposed on an operator when a notice is varied. Furthermore, Amendment 256 would provide for judicial commissioner authorisation when a variation adds obligations or steps to the notice, and when the notice is varied so that it imposes obligations in relation to additional services provided by the operator to its customers.

Amendment 257 makes it clear that the judicial commissioner's specific role in the approval process when a notice is varied is the same as that detailed in Clause 230 in relation to the giving of notices. In mirroring the process for giving notices, Amendment 258 also ensures that the operator may refer the notice as varied to the Secretary of State for review. The Secretary of State can confirm, vary or revoke the notice following a review, but any confirmation or variation would require the approval of the Investigatory Powers Commissioner. I hope that noble Lords will agree that these proposed changes would further strengthen the safeguards in Part 9 and, accordingly, I invite the House to support them. I beg to move.

Amendment 247 agreed.

Amendments 248 to 250

Moved by ***Earl Howe***

248: Clause 228, page 180, line 19, leave out from "But" to "to" in line 20 and insert "the Secretary of State may not give any telecommunications operator a national security notice the main purpose of which is to require the operator"

249: Clause 228, page 180, line 20, leave out "is required under any of the following enactments" and insert "under a relevant enactment is required.

( ) In this section "relevant enactment" means"

250: Clause 228, page 180, line 29, at end insert—

"( ) Conduct required by a national security notice is to be treated as lawful for all purposes (to the extent that it would not otherwise be so treated)."

Amendments 248 to 250 agreed.

Clause 229: Technical capability notices

Amendment 250A

Moved by ***Lord Paddick***

250A: Clause 229, page 180, line 46, at end insert—

"(c) specifying the distinct service or product to which the notice applies"

Lord Paddick: My Lords, Amendments 250A and 251A, in my name and that of my noble friend Lady Hamwee, relate to technical capability notices through which the Secretary of State can require an operator to have a capacity to provide any assistance necessary that might be required to give effect to the powers under the Bill. We have received representations on behalf of operators asking that those notices should be specific about the distinct service or product to which the notice applies, rather than a blanket, "You must have the capability to do anything we may require you to do under the powers contained in legislation". Amendment 250A is intended to have that effect, while Amendment 251A tries to limit the scope of technical capability notices. The power to issue a technical capability notice applies to any provider capable of being considered a telecommunications provider under the very broad definitions in the Bill. It would not be proportionate or necessary for this power to be so broad. The amendment aims to narrow the definition to exclude services that are not primarily communications services, even when there may be a communications element. Whether the wording of our amendment achieves that is a matter for debate, but that is what is intended. I beg to move.

Lord Rooker: Could the noble Lord list the operators to which he referred?

Lord Paddick: I can certainly tell the noble Lord that Yahoo! was one of the operators, but I do not have a list to hand.

Earl Howe: My Lords, Amendment 250A would define a technical capability notice as,

"specifying the distinct service or product to which the notice applies".

I do not believe this amendment is necessary. The safeguards that apply to the giving of a notice under the Bill already ensure that a technical capability notice cannot be of a generic nature. I will not go into detail here about the lengthy process that must be undertaken before a notice can be given; we have discussed them at length previously and we will undoubtedly review them again shortly during our discussions on encryption. But it might be helpful for me to summarise.

Before giving a notice, the Secretary of State must consult the company concerned. This process will ensure that the company is fully aware of which services the notice applies to. The decision to issue a notice must be approved by the Secretary of State and a judicial commissioner. The obligations set out in the notice must be clear so that the Secretary of State and judicial commissioner can take a view as to the necessity and proportionality of the conduct required. As I have already mentioned, we propose a similar role for the judicial commissioner when a notice is varied. The operator may raise any concerns about the requirements to be set out in the notice, including any lack of clarity regarding their scope, during the consultation process. The operator may also seek a formal review of their obligations, as provided for in Clause 233. The safeguards which apply to the giving of a notice have been strengthened during the Bill's passage through Parliament, and will ensure that the regime provided for under the Bill will be more targeted than that under existing legislation. It is for these reasons that I consider the amendment unnecessary.

Amendment 251A seeks to narrow the category of operators to whom a technical capability notice could be given. This change would exclude operators that provide services that have a communications element but are not primarily a communication service. This amendment, which has already been discussed in the Commons, is also unnecessary and, in my view, risks dangerously limiting the capabilities of law enforcement and the security and intelligence agencies. We are aware that the manner in which criminals and terrorists communicate is diversifying, as they attempt to find new ways to evade detection. We cannot be in a situation where terrorists, paedophiles and other criminals can use technology to escape justice. As David Anderson said,

"no-go areas for law enforcement should be minimised as far as possible, whether in the physical or the digital world".

It is important that the Government can continue to impose obligations relating to technical capabilities on a range of operators to ensure that law enforcement

[Earl Howe]
and the security and intelligence agencies can access, in a timely manner, communications of criminals and terrorists using less conventional services, such as those offered by gaming service providers and online marketplaces. It may be appropriate to exclude certain categories of operators from obligations under this clause, such as small businesses, but it is our intention to use secondary legislation to do so. It would not be appropriate to impose blanket exemptions on services that have a communications element but are primarily not a communication service, since to do so would make it clear to terrorists and criminals that communications over such systems could not be monitored.

For all the reasons I have set out, I hope that the noble Lord, Lord Paddick, will feel able to withdraw his amendment.

Lord Beith (LD): Before the noble Earl sits down, I refer to a point which at least needs to be borne in mind in drafting regulations. In most circumstances, if the Government impose upon a business an obligation of some kind, and behave totally unreasonably in doing so—or the business thinks that the Government are behaving unreasonably—the matter will end up in public discussion and the company has the weapon of saying to the public at large, "The Government are asking us to do something unreasonable". That must not happen in these circumstances because clearly secrecy must be maintained. Therefore, the company is in a weaker position than it would be in the normal exchange between government and business. I hope that Ministers will recognise that fact.

Earl Howe: With the leave of the House, I am grateful to the noble Lord for raising that point, which I think will come up in the next group of amendments when we discuss encryption because it is centre stage in that issue. He is absolutely right and I hope that I can assuage his concerns in the next debate.

Lord Paddick: I am very grateful to the Minister, particularly for his explanation around Amendment 251A. I completely accept that the whole range of ways in which people can communicate potentially needs to be covered. I am encouraged by the fact that there may be some exceptions in secondary legislation. It is unfortunate that we do not have sight of that before I withdraw this amendment but life is like that.

Bearing in mind the fact that the Minister did not articulate any downside to Amendment 250A, I wonder why the Government will not accept it, given that it appears not to limit the Government's action in any way. However, at this stage, I beg leave to withdraw the amendment.

Amendment 250A withdrawn.

Amendment 251

Moved by ***Lord Harris of Haringey***

251: Clause 229, page 181, line 32, at end insert—

"( ) For the purposes of this section, "electronic protection" does not include electronic protection applied directly by the communications device or operating system of the end user which has the effect of encrypting the communications data in transit such that the relevant telecommunications operator does not have a means to access the associated communications data or content."

Lord Harris of Haringey: My Lords, noble Lords who have followed my limited contributions to the Bill will know that I take a fairly robust approach in support of what the Government seek to do in it. Indeed, they may even be slightly perplexed that I have tabled this amendment, which is supported by the Liberal Democrat Front Bench, given the slightly testy exchanges that have occurred once or twice during the passage of the Bill. However, my philosophy throughout has always been clear—namely, that by and large this Bill is needed to update current legislation and to protect the public. However, all the measures have to be tested in terms of the balance that they strike between protecting the public and their potential invasion of privacy. We have debated that issue but in this case the disbenefits I am concerned about are the extent to which what the Government may be trying to do—the Minister will no doubt explain what that is in more detail in a few minutes—under the Bill as drafted will weaken the security that people would otherwise have.

The Bill provides the Home Secretary with the power to require a communications provider to install some sort of technical capability to provide data on request, including where those data would otherwise be encrypted and are therefore not so easily available. The Bill includes an impressive array of safeguards. The Home Secretary is required to apply a series of tests before they make a decision to serve an order on a communications provider, and a process of consultation and discussion has to go forward. Those measures are all designed to ensure that not only is the Home Secretary properly informed in making that judgment but using the power is practical and reasonable. Indeed, the Bill emphasises the importance of the test of something being reasonably practical and technically feasible. I have asked for an explanation of the precise distinction between reasonably practical and technically feasible. I accept that there may be a distinction.

A whole series of tests applies under those circumstances but we do not know how those tests might be applied in future or what the Home Secretary might decide. Therefore, we cannot know how a future Home Secretary, or the present Home Secretary, would interpret what is and is not practicable and reasonable. In particular, we face an ambiguity—at least I think there is an ambiguity here—over what it will mean for end-to-end encrypted services. End-to-end encrypted services allow an end-user to send a message via a particular service which can be opened and read only by the person to whom it is sent. That is an important reassurance which we would all like to have in terms of our private communications. The company that conveys that message to the other person—the company in the middle—has no ability to see that message. The communications provider has provided that as a service because it is believed that that is what customers want.

Not all communications providers do that. Some provide a service where it is clear—it says so on the tin—that they will have the option to be aware of what is in the message because they use that to sell advertising. However, not all communications providers operate

on that basis. The purpose of that encryption arrangement is to ensure that the data are protected by means of encryption against outsiders looking at them. The encryption key is held only by the person who sends the message and the person who receives it. Nobody else in between has that capacity. The potential implication of that is that the communications provider cannot find a way to discover the content of such a message, even if it wanted to and even if required to do so by the Government.

6.15 pm

Let us suppose that for some bizarre reason I wanted to send an iMessage to the noble Lord, Lord Paddick. If I did that in the normal way, it would be an encrypted message that Apple would not be able to read. As I am cautious about losing stuff, I might copy such an iMessage to iCloud. If I copy it to iCloud, the encryption key will be sent not just to the noble Lord, Lord Paddick, but also to Apple. It could be any of the other providers, I have just used that example because I have an iPhone. I do not know what phone the noble Lord, Lord Paddick, has and I do not particularly wish to. However, the point is that Apple could access that message in that particular example only when I had elected to copy it to iCloud, whereas if I sent it just to the individual, that would not be possible.

The question then arises of what the clauses we are discussing are intended to achieve in terms of technical capability notices. Is it the Government's intention to require a communications service provider, who provides an end-to-end encrypted service which otherwise the Government could not access, to create a capacity to enable the latter to read that message if the provider has received a technical capability notice? I assume that the Government do not want this to happen because they have said very clearly on a number of occasions that they believe encryption is important to people's confidence in conducting e-commerce and in maintaining their privacy. Therefore, the Government believe that it is a good thing. Ministers have repeatedly said that encryption is important. Therefore, is the intention of these clauses to enable the Government to say, "Ah, yes, but—we would like to be able, under very limited circumstances which have passed all the tests, to require a communications service provider to build something, which it would not otherwise have, to break into those communications and to unencrypt them?" I assume that this would be done only under the most extreme circumstances and with very good reasons.

It is extremely important that this point is clarified. The purpose of the amendment is to make it explicit that the Government are not requiring a communications service provider to build something new which enables the former to get at the encryption keys—perhaps when they produce the next version of that particular communications method—or to build something which enables them to get into that. That is an extremely important issue to clarify but at the moment the Bill is ambiguous on it.

If that ambiguity continues, that is bad for innovation and it is certainly bad for consumer confidence. There is a danger that it creates a general weakening of encryption. Once you create that mechanism, even if for the best reasons and within the heart of a communication service provider, you have weakened the nature of that end-to-end encryption. That means that that will become of interest, not just to the people for whom the communication is intended and the person sending it, or indeed to the communication service provider, but to all sorts of other people. It could be a hostile Government or cybercriminals, who will say, "We know that some mechanism is maintained by the communication service provider that can get at that encryption process", and they will target it. The mere fact of having created a door which can be opened will mean that other people rather than just those who think they have the right to do so will try to open it. Therefore there is a general potential weakening of encryption, with potential unintended consequences, and cybercriminals or hostile Governments could target that weakness.

If we say, "This is all right for us, because we have a benign Government with a legislative framework which provides robust safeguards, so this power will not be abused", the implication is that in other countries, which perhaps do not have such a robust framework, the precedent is difficult to set. They will say to the communication service providers, "You provide it to the United Kingdom Government, and we know you've got it, because you've built it into your systems worldwide. We want it for our nation state, and we'll let you know the circumstances in which you should make that available as regards our legislative provision". We are setting a dangerous international precedent.

It has been put to me that all that will happen is that those who want to use it for nefarious purposes will simply switch to another service. That is true of everything we have talked about in these circumstances. However, we need to take seriously the danger that the most used services in particular will weaken the encryption process. We have to be clear that that is the Government's intent, why it is their intent, and whether they have considered the potential downside of doing so. We have to be clear that if there is a reduction in the public confidence in the security of their communications, that will not be good for the economy, e-commerce, trade and everything else. It also plays right into the hands of those who believe that the Bill is simply some dreadful plot by the noble Lords opposite or the Government they represent to pry into the private details of every single one of us. I do not believe that that is the case—it is possible that one or two other people do—but it seems that the Government are playing right into their hands by looking at this.

The purpose of this amendment is simply to put in the Bill the provision that you are not asking the communication service providers to build something which at the moment they cannot do, and you are also not requiring them, next time they produce a messaging system or whatever else it might be, to put in a back door which can be opened in this way. I beg to move.

Lord Paddick: My Lords, I will speak to our Amendments 252 to 254 and the other amendments in this group. To save the noble Lord, Lord Rooker, having to get to his feet, this one is from Apple.

As the noble Lord, Lord Harris of Haringey, just outlined, it is essential that end-to-end encryption is not compromised by technical capability notices.

[Lord Paddick]

I anticipate that the Minister might say that Clause 231(3)(c) covers this in that it would not be technically feasible for the operator to remove electronic protection of this nature, but we support this amendment and believe that it needs to be explicit in the Bill. However, we do not believe that this amendment covers other forms of encryption. Our Amendment 252 is intended to protect UK operators from the real or perceived disadvantage they would be placed under if technical capability notices required them to make modifications that would make their product or service less secure than overseas operators, who may not be subject to or may refuse to comply with a similar technical capability notice.

Similarly, Amendment 253 is intended to prevent a technical capability notice stopping UK operators from innovating to improve the levels of security or encryption provided by their products and services in a way that would disadvantage them against overseas operators, which may not be subject to or refuse to comply with a similar technical capability notice.

Amendment 254 is intended to deal with the criticism of our amendment in Committee by the Minister, who said that he believed that it,

"would remove the Government's ability to give a technical capability notice to telecommunications operators requiring them to remove encryption from the communications of criminals, terrorists and foreign spies".—[*Official Report*, 13/7/16; cols. 272-73.]

This new amendment makes it clear that technical assistance can be given to enable interpretation and deciphering provided that it does not open the door to unauthorised access to encrypted materials by criminals, terrorists and foreign spies—essentially, what the noble Lord, Lord Harris, just said.

Amendment 252A, in the name of my noble friend Lord Strasburger, is an attempt to combine all the other amendments in this group into a much better-worded amendment. I look forward to hearing from him why this might be the case.

Lord Strasburger (LD): My Lords, I shall rise to that opportunity. Amendment 251, in the name of the noble Lord, Lord Harris, and my noble friends Lord Paddick and Lady Hamwee, addresses one particular kind of encryption—namely end-to-end encryption—and it is very good as far as it goes, which is end-to-end encryption. My own Amendment 252A is also in this group and is complementary to Amendment 251. It is, in my humble opinion, a neater way of dealing with encryption that is not end-to-end encrypted than the combination of the other amendments in this group: Amendments 252, 253 and 254. It is an alternative to them.

We have been around the block many times on the subject of encryption in the context of Clauses 229 to 231. It has come up several times in our debates on the Bill, as well as in questions in this House and in the Joint Committee on the Bill. Yet we are no closer to a clear and unambiguous understanding of the Government's position on this vital issue, as the noble Lord, Lord Harris, has so eloquently said.

It might help if we start from common ground. I doubt that any noble Lord, myself included, would deny the authorities the option of requiring an operator to decrypt a communication where: the operator already possesses the capability to do so; the sender or receiver of the communication is genuinely suspected of committing or planning a serious crime; and the appropriate process has been followed and the action has been judged necessary and proportionate by a judicial commissioner. I do not think that anybody would argue about that.

I believe there is more common ground. Ministers have repeatedly confirmed that the Government fully accept that many uses of the internet that are now an essential part of everyday life, both for individuals and for large organisations, cannot possibly continue to happen without the security provided by unbreakable encryption.

If we take those two points as read, we are left with two questions about what happens if the operator is not able to decrypt the communication. The first is: should the Secretary of State be able to force an operator to redesign its product so that in future its encryption has a weakness that permits the operator, or perhaps GCHQ, to read a suspect's messages? The other question is: should the Secretary of State have the power to prevent an operator introducing new or modified encryption services which neither the authorities nor the operator can break? The answer to both those questions is an unequivocal, "No, the Secretary of State should not have those powers", and noble Lords will be hard pressed to find a single cryptography specialist who has a different view. If the Government concur, as I hope they do, they should have no problem accepting Amendments 251 and 252A, which would remove the ambiguity in the current drafting.

6.30 pm

We need clarity because encryption is either secure or it is not. Any weakness or back door in an encryption system, whether mandated by government or due to an accidental error by the author, is available to be found or stolen and used for nefarious purposes. This could be done by large hacking teams working for a hostile state, a criminal gang in eastern Europe or a 13 year-old geek operating from his bedroom in Scunthorpe, and the damage could be immense. It is not possible for a weakness to be inserted in such a way that it is available to the good guys and, with any certainty, not to the bad ones. It is like hiding the front-door key under a rock and hoping that the burglar does not look under that particular stone. So the purpose of these amendments is to ensure that our country's use of the internet, for all its purposes, cannot be endangered by gaps in its security.

There is another important unintended consequence that Amendment 252A would prevent, and that is the serious risk of damage to the business of the UK's very successful and growing data encryption industry. For its clients, the strength of the security is paramount, and even just the possibility that the encryption product may have been degraded as a result of a secret government diktat under Clause 229 would be enough to drive the customers to competitors who operate in other countries where no such risk exists. The only way for British companies to mitigate that danger would be for them to move their business to a country where government-mandated degradation of security was

not possible. Relocation is what many of these companies are already considering if Clauses 229 and 231 pass unamended.

I should mention in passing that the security and intelligence services are less vexed than one might think about the increasing use of encryption. It does not prevent them seeing the communications data—if you like, the envelope around the letter—which are not encrypted. These usually reveal what they want to know—namely, who is talking to whom and when and where—and communications data are much easier for their computers to process than the content. If GCHQ needs to see unencrypted content, it can usually do that without decrypting it itself by hacking into either the sender's or the receiver's phone or computer and looking at it there unencrypted.

In summary, I hope the Government will be able to confirm that they accept Amendments 251 and 252A. These would remove the uncertainty that exists in the current drafting of the Bill about whether operators can be forced to vandalise the security of their own products to the detriment of all internet users and the UK tech industry. I look forward to hearing the Minister's response.

Lord Rooker: My Lords, if I could be convinced that the same rules applied everywhere on the globe—because we are talking about a global function—in respect of the rule of law, freedom, transparency and privacy protection, then I might have a bit of sympathy with the business operators, as we will call them.

I had the privilege of being among those serving on the RUSI panel. We had a discussion with the providers, but they did not all want to come and sit round the table at the same time—I recall two or three sessions—because they are competitors. We put it to them—it was not original; it had come up elsewhere—that not one of these companies, whether Apple, Google, Facebook, Twitter, Yahoo or Microsoft, would ever have been able to start what is now their global business in countries such as Russia, Iran and China. Yet they have become global and make enormous profits, although I will not go into the issue of them paying their taxes.

These providers hide behind the fact that the countries where they are able to start and function have the rule of law and are democracies where you can challenge Governments in the courts and get redress, yet they then go and operate in countries where they cannot do that. If they all said, "When we operate in China, we're going to produce all our phones fully encrypted, exactly as we do for everybody else. The Chinese Government are allowing us to close end to end. They don't want to know what their citizens are saying", then fine, but I do not believe that that is the case, and that is part of the problem.

My noble friend Lord Harris touched on the issue of other Governments, but we can legislate only for the UK. I fully understand that, yet half of an email sent from my office upstairs to a colleague here might be split and end up travelling through the rest of Europe or America or half-way round the world. That is how the system works. Just because you are emailing someone in this country from within this country, you cannot guarantee that the entire message will stay in this country while it is being whizzed round the world. The system does not work as I originally thought it did. So we can legislate only for this country and messages get split up around the world.

The fact is that the business plans and business operations of these companies depend on open, transparent and democratic countries with the rule of law, yet they are willing to work in countries where there is no rule of law and where there are corrupt regimes, such as in Russia, or undemocratic regimes, as in China. These are countries with huge populations and the companies can do business there according to a different business plan from the one that applies here. From the point of view of those who are there to protect us, that has to lead to a suspicion that at some point we might need a bit more information than we have and that we might need to ask for that to be provided.

I take second place to no one on the protection of privacy, but the fact is that you cannot discuss this issue just in the context of the UK or Europe; it is global, and the rules do not apply equally across the globe. If we take that on board, I think we ought to have a fair degree of sympathy with how the Government will operate these measures.

I have listened to other people and have read more about this matter since finishing our work on the RUSI panel, and the fact is that there is a great reluctance to have these powers. In a democracy there is an incredible reluctance for private information to be treated in this way, but at the end of the day there will be proportionality and our people will be tested on the need for these powers. One of the raisons d'être of the Bill is to put in second and third checks, so those with the powers will be watched and the watchers will be watched, and that is how we can give the public confidence. I do not think that we ought to write the Bill to suit the business operators' original business plans, because they are not implementing them on an equal basis across the globe. Therefore, I hope that the Government will reject these amendments.

Lord Harris of Haringey: Before my noble friend sits down, to be honest I think that he has slightly misunderstood the point that has been made. I am not putting this forward because of the business models of particular companies; I am proposing it because of the inherent weakness that could conceivably be created. His argument, if I understood what he just said, is that because Russia or China may require, or may force because the business there is so valuable, a communications service provider to put in one of these back doors, therefore we need to have the same facility. The point is that, because it is a global provision, if a back door is built in—because Russia or China or wherever else has demanded it—then a technical capability notice would operate because the operator would have that existing facility. That is precisely the circumstance in which a technical capability notice could be served. This amendment seeks to exclude a requirement from our Government that it should be created at our behest, which other people would then use.

Lord Rooker: I take on board what my noble friend is saying. I fully accept the distinction he makes but, basically, although I am a customer of some of these

[LORD ROOKER]
companies, I do not trust them—they will tell us that this has been built in and is secure, but do deals with those other regimes.

Lord Evans of Weardale (CB): My Lords, there have not been very many points in the course of this legislation on which I have agreed with the noble Lord, Lord Strasburger, but on this point I do. Amendment 252A raises a very interesting and important point.

Although I am absolutely in favour, as you would imagine, of the Government having the opportunity to access the communications of anybody who is a threat to us—due to terrorism, criminal activities or anything of that sort—there is a competing national security issue here of this country having effective cybersecurity. We have seen the way in which hostile Governments have been seeking to intervene in the American elections, and we have seen all sorts of attempts by hostile states, criminal groups and others to use cyber weaknesses to take forward hostile agendas. Therefore, there is a genuine national security interest in ensuring that, as far as we can, our citizens can communicate securely and privately when they are not going about mischievous business.

The idea that we should take into consideration the requirement not to place non-targeted customers or others at additional security risk is an entirely legitimate one, and I am very interested to hear how the Minister would want to interpret this. We have competing national security issues here and it is a point well made.

Baroness Hayter of Kentish Town: My Lords, we have had some rather good discussions with the tech companies. In Committee, we put in some of the amendments that they suggested to us, and some of the government amendments we have been dealing with over the past few days reflect that. I thank the tech companies for their very responsible attitude in continuing discussions with the Government over this period. Certainly with us they have been open, flexible and fairly straight as to what is possible and what the dangers are for them—for example, and as we have discussed, whether a weakness in end-to-end encryption could actually undermine the security that banks and others rely on in their systems—and for their clients, public confidence and national security. The companies recognise that they have a duty of care and loyalty to their customers, while fully respecting the law of the land in which they operate and the legal demands on their staff, wherever they are located.

In their discussions with us, companies have sought clarity that they will not be asked, effectively, to create a new system that would breach end-to-end encryption. They need this clarity for their shareholders and customers' peace of mind because the reality is that they could never be forced to create a new computer program to hack their own security. I for one cannot imagine the noble Earl, Lord Howe, or anyone else standing over a hapless computer programmer shouting, "Break into it!", if that company did not want to do it or the computer genius was on a go-slow that day. The idea that you could force somebody to create a program that the company and the employee did not want to is probably not possible.

Given that, the reality is that the things the Government want to ask will happen only when there is a good working understanding between the security services and the company. Therefore, if the tech companies want this clarity as set out in Amendment 251—as we know they do—our interest is to hear from the Minister just what the obstacles are to giving them the clarity that they seek.

6.45 pm

Earl Howe: My Lords, I hope that the House will allow me to speak at somewhat greater length than usual in responding to these amendments. I recognise the concern that lies behind them and I also recognise that, although we debated the Bill's provisions on encryption in Committee, there is a need to correct a number of misconceptions that have been expressed and to set out the reality of the Government's position on encryption. I would also like to make clear what the provisions in the Bill do and, crucially, what they do not do, and to explain why these provisions are so important to our law enforcement and intelligence agencies. I hope that by, setting this out, I can reassure noble Lords that the amendments are not necessary.

As we have made clear before, the Government recognise the importance of encryption. It keeps people's personal data and intellectual property secure and ensures safe online commerce. The Government work closely with industry and businesses to improve their cybersecurity. For example, GCHQ plays a vital information assurance role, providing advice and guidance to enable government, industry and the public to protect their IT systems and use the internet safely. Indeed, the director of GCHQ said in March that he is accountable to the Prime Minister just as much, if not more, for the state of cybersecurity in the UK as he is for intelligence collection.

In the past two years, the security and intelligence agencies have disclosed vulnerabilities in every major mobile and desktop platform, including the big names that underpin British business. You do not have to take the Government's word for that. In September 2015, Apple publicly credited the information assurance arm of GCHQ with the detection of a vulnerability in its operating system for iPhones and iPads, which could otherwise have been exploited by criminals to disrupt devices and extract information from them. As a result, this vulnerability could be fixed.

The assertion that the Government are opposed to encryption or would legislate to undermine it is fanciful. However, the Government and Parliament also have a responsibility to ensure that our security and intelligence services and law enforcement agencies have the capabilities necessary to keep our citizens safe. Encryption is now almost ubiquitous and is the default setting for most IT products and online services. While this technology is primarily used by law-abiding citizens, it can also be used—easily and cheaply—by terrorists and other criminals. Therefore, it can only be right that we retain the ability, as currently exists in legislation, to require a telecommunications operator to remove encryption in limited circumstances, subject to strong controls and safeguards. If we do not provide for this ability, then we must simply accept that there can be areas online beyond the reach of the law where criminals

can go about their business unimpeded and without the risk of detection. That would be both irresponsible and wrong.

That is our starting principle, and it is one that we share with David Anderson QC. I have quoted this before, but he stated in his investigatory powers review, *A Question of Trust*:

"My first principle is that no-go areas for law enforcement should be minimised as far as possible, whether in the physical or digital world".

This principle was also shared by the Joint Committee on the draft Bill and the Science and Technology Committee, both of which recognised that, in tightly prescribed circumstances, it should remain possible for our law enforcement agencies and security and intelligence services to be able to access unencrypted communications or data. That is exactly what Clauses 229 to 234 of the Bill provide for: strong safeguards to ensure that obligations to remove encryption can be imposed only in limited circumstances and subject to rigorous controls.

Clause 229 enables the Secretary of State to give a technical capability notice to a telecommunications operator in relation to interception, communications data or equipment interference. As part of maintaining a technical capability, the Bill makes clear at Clause 229(5)(c) that the obligations that may be imposed on an operator by the Secretary of State can include the removal of encryption. Before a technical capability notice is given, the Secretary of State must specifically consider the technical feasibility and likely cost of complying with it. Clause 231(4) provides that this consideration must explicitly take account of any obligations to remove encryption.

The Secretary of State must also consult the relevant operator before a notice is given. The draft codes of practice, which were published on 4 October, make clear that should the telecommunications operator have concerns about the reasonableness, cost or technical feasibility of any requirements to be set out in the notice, which of course includes any obligations relating to the removal of encryption, it should raise these concerns during the consultation process.

We have also amended the Bill to make clear that the Secretary of State may give a technical capability notice only where he or she considers that it is necessary and proportionate to do so, and, under Clause 230, that decision must also now be approved by a judicial commissioner, placing the stringent safeguard of the double lock on to any giving of a notice to require the removal of encryption. Clause 2 of the Bill, the privacy clause, also makes explicit that, before the Secretary of State may decide to give a notice, he or she must have regard to the public interest in the integrity and security of telecommunications systems.

In addition, a telecommunications operator that is given a technical capability notice may refer any aspect of the notice, including obligations relating to the removal of encryption, back to the Secretary of State for a review. In undertaking such a review, the Secretary of State must consult the Technical Advisory Board in relation to the technical and financial requirements of the notice, as well as a judicial commissioner in relation to its proportionality. We have amended the review clauses in the Bill to strengthen these provisions further. Where the Secretary of State decides that the outcome of the review should be to vary or confirm the effect of the notice, rather than to revoke it, that decision must be approved by the Investigatory Powers Commissioner.

The Bill also makes absolutely clear that, in line with current practice, obligations imposed on telecommunications operators to remove encryption may relate only to encryption applied by or on behalf of the company on whom the obligation is being placed. That ensures that such an obligation cannot require a telecommunications operator to remove encryption applied by other companies to data transiting their network. As we have already outlined, we have also now tabled a government amendment that would further strengthen the Bill's provisions on technical capability notices. This amendment makes clear that the Secretary of State may vary a notice only where they consider that it is necessary and proportionate to do so. The amendment also makes clear that, in circumstances where a notice is being varied in such a way that would impose new obligations on the operator, the variation must be approved by a judicial commissioner.

Furthermore, obligations imposed under a technical capability notice to remove encryption require the relevant operator to maintain the capability to remove encryption when it is subsequently served with a warrant, notice or authorisation, rather than requiring it to remove encryption per se. That means that companies will not be forced to hand over encryption keys to the Government. Such a warrant, notice or authorisation will be subject to the double lock of Secretary of State and judicial commissioner approval, and the company on whom the warrant is served will not be required to take any steps, such as the removal of encryption, if they are not reasonably practicable steps for that company to take. So a technical capability notice could not, in itself, authorise an interference with privacy. It would simply require a capability to be maintained that would allow a telecommunications operator to give effect to a warrant quickly and securely including, where applicable, the ability to remove encryption.

That is an enormously long list of safeguards. Indeed, it is difficult to think what more the Government could do. These safeguards ensure that an obligation to remove encryption under Clause 229 of the Bill will be subject to very strict controls and may be imposed only where it is necessary and proportionate, technically feasible and reasonably practicable for the relevant operator to comply. Let me be clear: the Bill's provisions on encryption simply maintain and clarify the current legal position, and apply strengthened safeguards to those provisions. They will mean that our law enforcement and security and intelligence agencies maintain the ability to require telecommunications operators to remove encryption in very tightly defined circumstances.

I would also like to make absolutely clear what the Bill does not provide for on encryption.

Lord Beith: Could the Minister help those of us who are not deeply technical in these matters? We fear that circumstances by their nature cannot be technical and defined. In at least some cases, the consequences of serving a notice would be that the operator would have to create a significant weakness, which would apply far beyond the objective for which the notice

[LORD BEITH]
was being served, and the operator would have to say in future to its customers, "This system is not as strong as we would like it to be".

Earl Howe: We come back to the test of reasonable practicability here. I am about to come on to what the Bill does not provide for on encryption and I hope that this will help the noble Lord.

The Bill does not ban encryption or do anything to limit its use. The Bill will not be used to force providers to undermine their business models, to create so-called back doors or to compromise encryption keys. It will not be used to prevent new encrypted products or services from being launched and it will not undermine internet security.

Lord Harris of Haringey: I am very grateful for the detailed exposition that has been given. The Minister says that the Bill will not be used to do those things. Can he confirm that it cannot be used to do those things?

Earl Howe: My Lords, some noble Lords have suggested the Bill's provisions cause a weakening in encryption, which I think is the central point that the noble Lord is getting at. Many of the biggest companies in the world rely on strong encryption to provide safe and secure communications and e-commerce, but retain the ability to access the content of their users' communications for their own business purposes, such as advertising, as we have heard. These companies' reputations rest on their ability to protect their users' data. This model of encryption can, and does, maintain users' security. I do not think that anyone would dispute that.

Before I come on to the individual amendments, it would be helpful to address a number of specific points that were raised in relation to encryption. There was a suggestion that a company should never be asked to do something that it does not already do. Such an approach would of course, at a stroke, remove our ability to use any of the powers in the Bill, including carrying out any interception of terrorists' and serious criminals' communications, because companies do not do this in the normal course of their business.

There was a suggestion that equipment interference would do away with the need for these provisions. It will not. Equipment interference is no substitute for having a company's assistance. Even if it were, there are only a very small number of very clever people who are able to carry out equipment interference. There will never be the capacity to deploy them on each and every operation.

Finally, there was a suggestion that encryption is not a problem for the security and intelligence agencies. The heads of those agencies have repeatedly made clear that ubiquitous encryption is one of the most difficult challenges they face.

I now turn to the individual amendments, because I hope that this will clarify the picture further. Amendment 251 seeks to preclude an obligation to remove encryption from being imposed under a technical capability notice in relation to end-to-end encrypted services. I hope that the points I have already made make clear why the proposed amendment is not necessary and indeed why it is not desirable. As I have set out, the Government recognise the vital importance of encryption. Nothing in the Bill does anything to limit its use, and that of course includes the use of end-to-end encryption. But I have also set out the dangers of creating a guaranteed safe space online for those who would seek to do the public harm such as terrorists and other serious criminals, and I am afraid that that is exactly what this amendment would do. The amendment seeks to make explicit provision in law for there to be certain online services that criminals can use to go about their business unimpeded with no fear of being caught. That is not a position that any responsible Government or, I hope, Parliament could support.

What we must ensure is that the Bill enables us to work collaboratively with individual telecommunications operators to establish what steps are reasonably practicable for them to take, considering a range of factors including technical feasibility and likely cost. Any decision will have regard to the particular circumstances of the case, recognising that there are many different models of encryption, including many different models of end-to-end encryption, and that what is reasonably practicable for one telecommunications operator may not be for another.

As I have already said, this is not about asking companies to undermine their existing business models; it is about working with them to find a solution to ensure both that their customers' data remain secure and that their services cannot be exploited by individuals who pose a threat to the UK. So in answer to the question put by the noble Lord, Lord Harris, I can confirm that these provisions cannot be used to introduce back doors or undermine internet security.

7 pm

Amendments 252, 252A, 253 and 254 seek to prohibit the Secretary of State from imposing an obligation to remove encryption in certain circumstances, namely: where that obligation would have the effect of making communications or data less secure; where it would threaten or harm the operator's business operations; where it would prevent the introduction of new types or levels of encryption; or where it would make communications or data more vulnerable to unauthorised access. These amendments are simply not necessary.

As I have set out very clearly, the strict and robust safeguards in the Bill already ensure that obligations to remove encryption would not have the effect of reducing the security of the internet or of a particular telecommunications service. I will not set out those safeguards again except to reiterate that, before giving a technical capability notice, the Secretary of State and a judicial commissioner must specifically consider the public interest in the security and integrity of telecommunications systems. The Bill ensures that the Secretary of State must specifically consider the cost and technical feasibility of complying with an obligation to remove encryption as well as whether it is reasonably practicable. This ensures that such an obligation cannot threaten or undermine a company's business model and, as I have already made clear, there is nothing in the Bill that would limit the use of encryption or prevent a telecommunications operator from launching new encrypted services or products.

So for all the reasons I have outlined, these amendments are unnecessary and in some cases dangerous. They would undermine the important principle that there should be no guaranteed safe spaces online for terrorists and criminals to communicate. I hope that the noble Lord opposite is sufficiently reassured by what I have said to withdraw his amendment.

Lord Strasburger: My Lords, if the noble Earl is so confident that none of the unintended consequences listed in Amendment 252A can occur, and that the Government do not want them to occur, what is his objection to putting them into the Bill?

Earl Howe: We already have a wide range of safeguards which I have listed. I do not see that it is necessary to go down the road the noble Lord is advocating because of the dangers that I have pointed out. These amendments would create safe spaces which I am sure that neither he nor any noble Lord would desire to occur.

Lord Harris of Haringey: My Lords, I am enormously grateful to the noble Earl for his detailed response and for reiterating the welcome and voluminous safeguards that are set out in the Bill. They are important and valuable, and they give me confidence about the context of the whole Bill. However, the argument with which he concluded does not quite hold together and there is an elision between different issues. The noble Earl has given an absolute assurance, I think on the basis of a piece of paper that was handed to him, that it cannot be used to require a communications service provider to build a back door or to create one in a future area. But then he said that we must not put in the Bill something that creates a safe space. Either the Government's position is that this cannot be used to require a company to produce a back door, in which case the safe space exists and presumably the Government are not happy with their own legislation, or it is the case that the Bill could require a communications service provider to build such a back door.

We have already heard from the noble Lord, Lord Evans of Weardale, that what we are trying to do here is balance two national security concerns: the national security concern to prevent terrorism and so on and the national security concern about making it slightly easier for cybercriminals. These are very important issues. If the Government are clear that, as a result of the Bill, a technical capability notice could not require an operator to build a back door that would otherwise not exist, it is important to set that out in the Bill. If we are in a position where techUK says—as it has in the briefing it circulated to me and, I am sure, to other noble Lords—that this is ambiguous, perhaps it is the responsibility of the Government to remove that ambiguity and make the position clear. I do not really want to have to divide the House on this matter, so between now and Third Reading, is the noble Earl prepared to turn the unequivocal assurance he has given that it cannot be used in this way into an amendment to the Bill that will remove that ambiguity?

Earl Howe: With the leave of the House, I hope I can help the noble Lord on this because I do not believe that the Bill is contradictory. First, the term "back door" has been used, but I do not think that is a helpful or accurate way of describing the Bill's provisions. "Back door" is in everyone's judgment a loosely defined term. It is used incorrectly to imply that the Bill would enable our law enforcement, security and intelligence agencies to gain unrestricted access to a telecommunications operator's services or systems, thereby undermining the security of those services—to force that to happen. That is absolutely not the case. The Bill enables our agencies to require telecommunications operators to remove encryption themselves, only in tightly defined circumstances: where they have applied the encryption themselves; where it has been applied on their behalf; where it is reasonably practicable for them to remove it; and where doing so is required to comply with a relevant warrant, notice or authorisation.

I come back to the point I made earlier. This is about the Government being able to sit down with companies and reach agreement with them on the basis of what is reasonably practicable, affordable and so on. It would not be responsible for any Government to deny themselves the possibility of doing that and discussing what in all the circumstances is reasonably practicable for the company, and for the company to agree to do it.

Lord Harris of Haringey: Again I am grateful to the noble Earl. I do not think anyone here has misunderstood the point that this is not about giving the Government uninterrupted access. It is about requiring companies to create a facility so that if they are asked, after all the suitable warrants have been gone through and all the safeguards have been fulfilled, to gain information and pass it back to the Government. I accept that that is the position and that is what is intended here. However, the Minister has still not been unequivocal on whether technical capability measures could require such a facility to be created, so that, in those circumstances and with all those safeguards in place, something could be done. It is a critical issue that we need to clarify. Otherwise, we do not know where we stand as far as the amendment is concerned. The Minister needs to provide the House and the IT industry with as much clarity as he can on this point, because the danger is that it will become the subject of continual argument.

Were the Bill to be amended by any of the amendments in this group, the Government would still have the option to say that they were minded to serve a technical capability notice on a particular company. That would then trigger a series of discussions, because it is what the Bill provides for, and a communications service provider might come back at that point and say, "Look, we literally cannot do it. We do not have the facility". However, it is not clear whether the Government could none the less say, "Well, we understand that, but we are requiring you to do it". The question then is: what is or what is not feasible? I happen to believe that some of the biggest communications service providers in the world have more computing expertise than any nation state. If they are told, "You are legally required to do this", they could do it; they could find a way of making it happen. We have to be explicit as to what the Government's expectation is. Are they saying, "No, that is not what we are requiring", or are they saying, "Well, we might"? If they are saying, "We might", that

[LORD HARRIS OF HARINGEY]
clarifies the position, if not helpfully. If they are saying, "No, we are not", which is what the Minister said earlier, perhaps we could put that in the Bill—if not in the form of words proposed, then in some form of words that the Government could craft between now and next week. That would be a helpful way forward and provide absolute clarity as to the extent to which technical capability notices could be served. If I am not able to get that assurance from him—I appreciate that bits of paper have been flying backwards and forwards between him and the Box—we are in a very difficult position.

Earl Howe: I can state categorically to the noble Lord that it is absolutely not the case that the Bill would force a company to insert a back door, thereby undermining internet security. We might ask a company in certain circumstances to decrypt particular data if it was reasonably practicable and feasible for them to do so.

Lord Harris of Haringey: My Lords, I understand that that is the case; that is, if they have the encryption key—we will not use "back door"; we will find another form of words—and the capability to do it, and it is not too complicated and all the relevant warrants are in place, yes, they will do that. As I understand it, most tech companies are perfectly understanding of that and willing to do it. The question is whether, if the Government were presented with a situation they were concerned about, they could say to one of the biggest communications service providers in the world, "We are asking you to build something which is not there at the moment, but we'll provide that facility for those circumstances that might arise in the future when we've gone through all the relevant warrants and so on". I am looking for an assurance from the Minister that that is not sought here, because of the dangers that we have already discussed. If he wishes, I can reiterate the question to give the Minister the opportunity to read the piece of paper that has just arrived.

7.15 pm

Earl Howe: Of course, a technical capability notice can require a new capability to be built; that is what they are there for. If it was neither practicable nor feasible, they would not have to do it. The problem here is that it is very difficult to generalise, because any decision about these things would have to have regard to the particular circumstances of the case. As I said, there are many different models of encryption, including many different models of end-to-end encryption. Any decision has to recognise that what is reasonably practicable for one telecommunications operator may not be for another. That is why I have referred repeatedly to the need for the Government and industry to have that easy interchange which they do at the moment. It is important to emphasise that these powers already exist in law today. We should not do anything that undermines the basis for the constructive discussions that we are having.

Lord Harris of Haringey: The Minister reminds us that the ideal arrangement is one of easy interchange and discussion—I understand that that carries on and works very well. He is right to say—this is why the wording of the current legislation is ambiguous and therefore a problem—that building a technical capability could mean simply putting in a piece of equipment, which means that, at the point at which the Government ask, having gone through all the voluntary processes, it is quite a straightforward matter to provide the information that the Government have legitimately and lawfully requested. That is one definition of technical capability.

What I want to know is whether "technical capability" could apply to a very secure end-to-end encryption process which no communications service provider could break but where, if they devoted thousands of person hours in California or wherever they operate from, they could develop something which might do that. If that is what the Bill is saying, we need to know.

Earl Howe: That would not be reasonably practicable in that particular example.

Lord Harris of Haringey: I accept that it would not be reasonably practicable; it would also be very expensive—as I understand the Bill, the Government would have to pay for it and I am sure that technical experts in California or wherever might be very expensive. If that is the case, and if it is not possible to write it into the Bill—I would have thought it could be—it would be helpful for the Minister to write and make very clear what the Government's intentions are in that regard and confirm that such circumstances are precluded by the Bill. If the Minister is prepared to do that, I am prepared not to press the amendment to a vote.

Earl Howe: I think I have made the Government's position as clear as I possibly can and I am not sure what I can do to amplify the remarks I have already made. While I want to be as helpful as possible to the noble Lord, I am struggling to see how a letter from me would make the position clearer.

Lord Harris of Haringey: I understand the Minister's dilemma and I am sure that a letter from him to me would have far less force than the words appearing in *Hansard*. I appreciate that the courts can look at the debates in *Hansard* to try to interpret them. However, I ask that the Minister spends the next few days just thinking about some further modification to the Bill to make sure that this ambiguity, which I think genuinely exists—because techUK tells me so—is cleared up. On the basis that I am sure he will spend his waking hours between now and next Monday thinking about precisely these matters, I beg leave to withdraw the amendment.

Amendment 251 withdrawn.

Amendment 251A not moved.

Clause 231: Further provision about notices under section 228 or 229

Amendments 252 to 254 not moved.

Clause 232: Variation and revocation of notices

Amendments 255 to 257

Moved by ***Earl Howe***

255: Clause 232, page 184, line 2, leave out "only if" and insert "given to a person only if—

(a) the Secretary of State considers that the variation is necessary in the interests of national security,

(b) "

256: Clause 232, page 184, line 4, at end insert ", and

(c) if the variation would impose further requirements on the person, the decision to vary the notice has been approved by a Judicial Commissioner (but see subsection (4B)).

(4A) The Secretary of State may vary a technical capability notice given to a person only if—

(a) the Secretary of State considers that the variation is necessary for securing that the person has the capability to provide any assistance which the person may be required to provide in relation to any relevant authorisation (within the meaning of section 229,

(b) the Secretary of State considers that the conduct required by the notice as varied is proportionate to what is sought to be achieved by that conduct, and

(c) if the variation would impose further requirements on the person, the decision to vary the notice has been approved by a Judicial Commissioner (but see subsection (4B)).

(4B) The condition in subsection (4)(c) or (as the case may be) subsection (4A)(c) does not apply in the case of a variation to which section 233(10) applies."

257: Clause 232, page 184, line 7, at end insert—

"( ) Section 230 (approval of notices by Judicial Commissioners) applies in relation to a decision to vary a relevant notice (other than a decision to which section 233(10) applies) as it applies in relation to a decision to give a relevant notice, but as if—

(a) the reference in section 230(2)(a) to the notice were to the variation, and

(b) the reference in section 230(2)(b) to the notice were to the notice as varied."

Amendments 255 to 257 agreed.

Clause 233: Review of notices by the Secretary of State

Amendment 258

Moved by ***Earl Howe***

258: Clause 233, page 185, line 13, after first "section" insert "or section 234"

Amendment 258 agreed.

Clause 236: Review of operation of Act

Amendment 258A

Moved by ***Lord Paddick***

258A: Clause 236, page 186, line 24, after "period," insert "and thereafter at least once during each Parliament,"

Lord Paddick: My Lords, I shall also speak to Amendment 258B. The powers in the Bill are significant, as are the checks and auditing measures, but the Government accept, in providing for a review of the operation of the Act and in anticipating that a Select Committee of one or both Houses of Parliament will also want to look at the operation of the Act, that a full, independent review is both necessary and desirable. The Bill sets the initial period at five years and six months and requires the Secretary of State to prepare a report within six months of the initial period. These amendments would ensure that before any Government are held to account by the electorate at a general election, the electorate know what that Government have used the powers in the Bill for.

Amendment 258A adds to the requirement to produce a report within six months of the initial period that the report must be produced at least once during each Parliament. Amendment 258B reduces the initial period from five years and six months to two years and six months, to ensure that the actions of the present Government are clear to the electorate at the next general election, subject, obviously, to the current Government remaining in office for the full term. I beg to move.

Lord Rosser: There is obviously going to be a desire to know how the Act is operating and the Bill does provide for a report from the Secretary of State, but it is, let us just say, some time after the day on which the Bill becomes an Act. Assuming that the Government do not accept the amendment, I hope that in responding they will set out, or give some indication, of the bodies and committees which will look at how the Act is operating, including whether it is doing so in line with the terms of the Bill. In that, I include the codes of practice and, particularly in light of the last discussion we had, the statements on the record from the Government in the two *Hansard*s during the passage of the Bill.

Lord Murphy of Torfaen (Lab): My Lords, I shall add some points to what my noble friend has just said. During our rather long deliberations this evening and afternoon, I went to the Library to look up the definition of "draconian". It seems to me to be very harsh, very severe. Apparently, it goes back to ancient Greece, where Draco was the statesman who decided that every single crime would be dealt with by a death sentence. It is not a good description of the Bill and the shadow Home Secretary is unfair and, I think, mischievous in what she said, because the Bill is significant, extremely serious and very difficult. It tries to balance the importance of security in our country, which was discussed at some length today, and our liberties.

I have to say that in 30 years in Parliament I do not think I have seen a Bill which has been scrutinised quite as well as this—not just by the Joint Committee that we were on in November and December but by other committees as well and, indeed, what we have seen in this House and the House of Commons. Nevertheless, the Joint Committee, at the very end of its deliberations, knowing full well that there would be an enormous amount of scrutiny, looked at what could happen in terms of review of the Bill. The Information Commissioner, indeed, gave evidence to the Joint Committee indicating that he thought there

[Lord Murphy of Torfaen]
should be a sunset clause. The then Home Secretary, who has gone on to greater things, indicated that this was not appropriate, but the committee believed that parliamentary review of the operation of what will then be an Act should take place within six months after five years. That has been incorporated into the Bill and it is the most important type of scrutiny that could happen, because that would be a Joint Committee of both Houses of Parliament, one hopes, which could look at how the Bill has operated. The reason the Joint Committee said that was because of the hugely grave and serious nature of the Bill—not just because of the way it touches on the liberties of the subject, but protecting the subject as well.

Lord Keen of Elie: My Lords, we remain sympathetic to the desire for ongoing scrutiny of the Bill, and this is already provided for. In these circumstances we suggest that these amendments are not necessary. The Bill requires that the operation of the Act will be reviewed after five years, which is an entirely appropriate period. It is also consistent with the recommendation, as indicated, of the Joint Committee that scrutinised the draft Bill. We must ensure that, before a review takes place, all the Bill's provisions have been in effect for a sufficient period that a review is justified and can be meaningful. A review after three years, as provided for by Amendments 258A and 258B, runs the risk that this would not be the case.

We also fully expect the review after five years to be informed by a report of a Joint Committee of Parliament, in line with the recommendation made by the Joint Committee. In addition, concurrent with such a review the Intelligence and Security Committee of Parliament would have the opportunity to assess the more sensitive aspects of the operation of the Act. Let us remember that, in addition, the exercise of the powers provided for under the Bill will of course be subject to the ongoing oversight of the Investigatory Powers Commissioner, who will be obliged to make an annual report to the Prime Minister.

The Government have listened to the previous debates in Parliament and amended the Bill to ensure that the Investigatory Powers Commissioner must, in particular, keep under review and report on the operation of safeguards to protect privacy. Furthermore, the Investigatory Powers Commissioner's reports must be published and laid before Parliament, providing Parliament with ongoing scrutiny of the operation of the Act. Accordingly, I invite the noble Lord to withdraw the amendment.

Lord Paddick: My Lords, I am grateful to the noble and learned Lord for his explanation. We are still of the view that at least once every Parliament, before a general election is called, a Joint Committee of both Houses of Parliament, as suggested by the noble Lord, Lord Murphy, should look at what the Government have been up to during their time in office so that the electorate are fully aware of how the Government have used the Bill. However, at this stage I beg leave to withdraw the amendment.

Amendment 258A withdrawn.

Amendment 258B not moved.

Amendment 258C

Moved by ***Baroness Hamwee***

258C: Clause 236, page 186, line 28, after "particular" insert—

"(a) report on any review by the Investigatory Powers Commissioner on the compliance of—

(i) officers of the Security Service, the Secret Intelligence Service and the Government Communications Headquarters, and

(ii) members of the armed forces of the United Kingdom and officials of the Ministry of Defence so far as they engage in intelligence activities,

with guidance from time to time issued on the detention and interviewing of detainees overseas and on the passing and receipt of intelligence relating to detainees; and

(b) "

Baroness Hamwee: I apologise to the House both that this is a rather inelegantly presented amendment and that it comes at a rather odd point in the Bill, but it covers a matter that was brought to our attention only very recently. I put thanks on the record to the organisation Reprieve for spotting the point. It would more naturally have come with clauses we debated on Monday, but we did not want to table a manuscript amendment for that.

In 2013, the Intelligence Services Commissioner was given additional functions by the then new Section 59A of RIPA. The commissioner is required, so far as directed by the Prime Minister, to keep under review the carrying out of any aspect of the functions of the intelligence services, their heads and the Ministry of Defence and forces engaging in intelligence activities.

7.30 pm

In 2014 the then Prime Minister confirmed in a Written Statement that he had given the direction to put on a statutory footing,

"the Commissioner's role overseeing compliance with the Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees".

He commented that the oversight had begun in 2010 and reminded Parliament that in 2013 he was asked by the commissioner to issue this direction. He said in the Statement that he would do so,

"following the publication of the Intelligence and Security Committee's report into the murder of Fusilier Lee Rigby".

The committee had been,

"critical of the Secret Intelligence Service for the handling of allegations of Michael Adebolajo's mistreatment in Kenya, made during his interview by the police … on his return to the UK".

The then Prime Minister went on to say:

"The Intelligence Services Commissioner plays a crucial role as part of the oversight regime for the work of the Security and Intelligence Agencies … This Government has been determined from the outset to have greater clarity about what is and what is not acceptable when dealing with detainees held overseas by other countries".—[*Official Report*, Commons, 27/11/14; col. 49WS.]

That is why the guidance was published.

Clause 218 abolishes the offices of various commissioners, including the Intelligence Services

Commissioner, and repeals Section 59A of RIPA. In his annual report last year, the commissioner expressed concern that:

"The IP Bill does not make provision for oversight of the Consolidated Guidance under the proposed Investigatory Powers Commissioner".

Recommendation 96 of David Anderson's report, *A Question of Trust*, was that the new commissioner,

"should inherit the intelligence oversight functions of the ISCommr, including … oversight of the Consolidated Guidance … and … keeping under review the activities of the security and intelligence agencies or others engaging in intelligence activity, as directed by the Prime Minister under RIPA s59A".

The purpose of this amendment is to inquire on what basis that oversight is to be achieved. I beg to move.

Lord Keen of Elie: My Lords, this amendment is unnecessary. The Government have already made it clear that the new Investigatory Powers Commissioner will bring together the existing responsibilities of the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Chief Surveillance Commissioner. That includes oversight of the consolidated guidance on the detention and interviewing of detainees. In addition, the Investigatory Powers Commissioner will have a bigger budget and a dedicated staff of commissioners and inspectors, as well as independent legal advisers, to ensure that the highest levels of independent scrutiny are maintained. In these circumstances, I invite the noble Baroness to withdraw her amendment.

Baroness Hamwee: My Lords, I chose the last words of my remarks quite carefully because it is the statutory basis of the current arrangements that is so important, which is why we raised it at this—I acknowledge—late stage. Obviously, I am glad to have these assurances. They do not answer my question but that position is now on the record. I beg leave to withdraw the amendment.

Amendment 258C withdrawn.

Clause 238: Postal definitions

Amendment 259

Moved by ***Earl Howe***

259: Clause 238, page 189, line 31, after "be" insert "or is capable of being"

Amendment 259 agreed.

Clause 239: General definitions

Amendments 260 to 267

Moved by ***Earl Howe***

260: Clause 239, page 191, leave out lines 46 and 47

261: Clause 239, page 191, line 49, at end insert—

""premises" includes any land, movable structure, vehicle, vessel, aircraft or hovercraft (and "set of premises" is to be read accordingly),"

262: Clause 239, page 192, line 16, at end insert—

""source of journalistic information" means an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used,"

263: Clause 239, page 192, line 19, at end insert—

""statutory", in relation to any function, means conferred by virtue of this Act or any other enactment,"

264: Clause 239, page 192, line 28, at end insert—

""the Technology Advisory Panel" means the panel established in accordance with section (Technology Advisory Panel)(1),"

265: Clause 239, page 192, line 35, after "identify" insert ", or assist in identifying,"

266: Clause 239, page 192, line 36, after "identify" insert ", or assist in identifying,"

267: Clause 239, page 192, line 39, after "identify" insert ", or assist in identifying,"

Amendments 260 to 267 agreed.

Amendment 268

Moved by ***Earl Howe***

268: After Clause 239, insert the following new Clause—

"General definitions: "journalistic material" etc.

(1) The definitions in this section have effect for the purposes of this Act.

Journalistic material

(2) "Journalistic material" means material created or acquired for the purposes of journalism.

(3) For the purposes of this section, where—

(a) a person ("R") receives material from another person ("S"), and

(b) S intends R to use the material for the purposes of journalism,

R is to be taken to have acquired it for those purposes.

Accordingly, a communication sent by S to R containing such material is to be regarded as a communication containing journalistic material.

(4) For the purposes of determining whether a communication contains material acquired for the purposes of journalism, it does not matter whether the material has been acquired for those purposes by the sender or recipient of the communication or by some other person.

(5) For the purposes of this section—

(a) material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose, and

(b) material which a person intends to be used to further such a purpose is not to be regarded as intended to be used for the purposes of journalism.

Confidential journalistic material

(6) "Confidential journalistic material" means—

(a) in the case of material contained in a communication, journalistic material which the sender of the communication—

(i) holds in confidence, or

(ii) intends the recipient, or intended recipient, of the communication to hold in confidence;

(b) in any other case, journalistic material which a person holds in confidence.

(7) A person holds material in confidence for the purposes of this section if—

(a) the person holds it subject to an express or implied undertaking to hold it in confidence, or

(b) the person holds it subject to a restriction on disclosure or an obligation of secrecy contained in an enactment."

Amendment 268 agreed.

Clause 240: Index of defined expressions

Amendments 269 to 275

Moved by ***Earl Howe***

269: Clause 240, page 193, line 27, at end insert—

"Confidential journalistic material	Section (General definitions: "journalistic material" etc.)(6) and (7)"

270: Clause 240, page 194, line 20, at end insert—

"Journalistic material	Section (General definitions: "journalistic material" etc.)(2) to (5)"

271: Clause 240, page 194, leave out line 27

272: Clause 240, page 194, line 33, at end insert—

"Premises	Section 239 (1)"

273: Clause 240, page 195, line 9, leave out "74(8)" and insert "239(1)"

274: Clause 240, page 195, line 11, at end insert—

"Statutory (in relation to any function)	Section 239(1)"

275: Clause 240, page 195, line 14, at end insert—

"Technology Advisory Panel	Section 239(1)"

Amendments 269 to 275 agreed.

Clause 242: Regulations

Amendment 276

Moved by ***Earl Howe***

276: Clause 242, page 196, line 20, at end insert—

"( ) section 218(2A),"

Amendment 276 agreed.

Schedule 9: Transitional, transitory and saving provision

Amendments 277 to 280

Moved by ***Earl Howe***

277: Schedule 9, page 242, line 26, leave out "section 86(1) to (11)" and insert "sections 84(1)(b), (3A) and (7)(e), (Approval of retention notices by Judicial Commissioners), 86(1) to (11), (Approval of retention notices following review under section 86), 89(4)(b), (5A), (8A) and (9A) and 91(2)(de)"

278: Schedule 9, page 243, line 3, at end insert—

"but this is without prejudice to the continued operation of section 90(2) to (5) in relation to the notice."

279: Schedule 9, page 243, line 18, at end insert—

"_(1) Sub-paragraph (2) applies if any power to give, vary or confirm a retention notice under section 84 of this Act (excluding any power to vary a notice which has effect as such a notice by virtue of paragraph 3(1)) is brought into force without any requirement for approval by a Judicial Commissioner of the decision to give, vary or (as the case may be) confirm the notice.

_(2) The notice as given, varied or confirmed ceases to have effect (so far as not previously revoked) at the end of the period of three months beginning with the day on which the requirement for approval comes into force."

280: Schedule 9, page 243, line 42, after "operator" insert "(within the meaning given by section 27(3) of the Postal Services Act 2011)"

Amendments 277 to 280 agreed.

Clause 246: Minor and consequential provision

Amendment 281

Moved by ***Earl Howe***

281: Clause 246, page 199, line 2, at end insert—

"( ) In subsection (3) "enactment" does not include any primary legislation passed or made after the end of the Session in which this Act is passed."

Amendment 281 agreed.

Schedule 10: Minor and consequential provision

Amendments 282 to 293

Moved by ***Earl Howe***

282: Schedule 10, page 250, line 17, at end insert—

"Security Service Act 1989

In section 1(5) of the Security Service Act 1989 (meaning of "prevention" and "detection") for the words from "the provisions" to the end substitute "that Act"."

283: Schedule 10, page 250, line 28, at end insert—

"Intelligence Services Act 1994

In section 11(1A) of the Intelligence Services Act 1994 (meaning of "prevention" and "detection") for the words from "apply" to the end substitute "apply for the purposes of this Act as it applies for the purposes of that Act, except that for the purposes of section 3 above it shall not include a reference to gathering evidence for use in any legal proceedings (within the meaning of that Act).""

284: Schedule 10, page 251, line 13, at end insert—

"Police Act 1997

In section 133A of the Police Act 1997 (meaning of "prevention" and "detection") for the words from "the provisions" to the end substitute "that Act"."

285: Schedule 10, page 251, line 34, at end insert—

"(1) Section 49 (investigation of electronic data protected by encryption etc: powers under which data obtained) is amended as follows.

(2) In subsection (1)(b) after "communications" insert "or obtain secondary data from communications".

(3) After subsection (9) insert—

"(9A) In subsection (1)(b) the reference to obtaining secondary data from communications is to be read in accordance with section 16 of the Investigatory Powers Act 2016.""

286: Schedule 10, page 252, line 37, leave out from "(1)" to end of line 38 and insert "—

(a) for "23A" substitute "72 of the Investigatory Powers Act 2016", and

(b) for "or 32A" substitute "or section 32A of this Act"."

287: Schedule 10, page 253, line 34, at end insert—

"Regulation of Investigatory Powers Act 2000

59A_ The Regulation of Investigatory Powers Act 2000 is amended as follows.

59B_ In section 48 (interpretation of Part 2), in subsection (3)(c)—

(a) omit the "or" at the end of sub-paragraph (i);

(b) after sub-paragraph (ii) insert "; or

(iii) Part 5, or Chapter 3 of Part 6, of the Investigatory Powers Act 2016 (equipment interference)."

59C(1) Paragraph 2 of Schedule 2 (persons having the appropriate permission where data obtained under warrant etc) is amended as follows.

_(2) In sub-paragraph (1)—

(a) omit the "or" at the end of paragraph (a);

(b) after paragraph (b) insert "; or

(c) a targeted equipment interference warrant issued under section 101 of the Investigatory Powers Act 2016 (powers of law enforcement chiefs to issue warrants to law enforcement officers)."

_(3) In sub-paragraph (5), at the end insert "or under a targeted equipment interference warrant issued under section 101 of the Investigatory Powers Act 2016."

_(4) In sub-paragraph (6)—

(a) omit the "and" at the end of paragraph (b);

(b) after paragraph (c) insert "; and

(d) in relation to protected information obtained under a warrant issued under section 101 of the Investigatory Powers Act 2016, means the person who issued the warrant or, if that person was an appropriate delegate in relation to a law enforcement chief, either that person or the law enforcement chief."

_(5) After sub-paragraph (6) insert—

"(6A) In sub-paragraph (6)(d), the references to a law enforcement chief and to an appropriate delegate in relation to a law enforcement chief are to be read in accordance with section 101(5) of the Investigatory Powers Act 2016.""

288: Schedule 10, page 254, line 8, leave out ", or Chapter 3 of Part 6,"

289: Schedule 10, page 255, line 8, leave out from "dismissed)" to end of line 9 and insert "omit "under section 107(2),""

290: Schedule 10, page 255, line 31, at end insert—

"_(1) Section 64 (delegation of Commissioners' functions) is amended as follows.

(2) In the heading for "Commissioners' functions" substitute "functions of the Investigatory Powers Commissioner for Northern Ireland".

(3) In subsection (1)—

(a) omit "or any provision of an Act of the Scottish Parliament", and

(b) for "a relevant Commissioner" substitute "the Investigatory Powers Commissioner for Northern Ireland".

(4) Omit subsection (2)."

291: Schedule 10, page 255, line 36, after "substitute ""insert—

"(bza) the Investigatory Powers Commissioner for Northern Ireland carrying out functions under this Act"

292: Schedule 10, page 258, line 17, at end insert—

"Anti-terrorism, Crime and Security Act 2001	Section 116(3)."

293: Schedule 10, page 260, line 14, leave out "and (3)"

Amendments 282 to 293 agreed.

Clause 247: Commencement, extent and short title

Amendments 294 and 295

Moved by ***Lord Wallace of Tankerness***

294: Clause 247, page 199, line 5, leave out "(2) and" and insert "(1A) to"

295: Clause 247, page 199, line 7, at end insert—

"(1A) Sections (civil liability for certain unlawful interceptions) and (interception without lawful authority: awards of costs) come into force on the day following that on which this Act is passed."

Amendments 294 and 295 agreed.

Amendments 296 to 300

Moved by ***Earl Howe***

296: Clause 247, page 199, line 12, leave out "and (6)" and insert "to (6A)"

297: Clause 247, page 199, line 14, after "revocation" insert "made by this Act"

298: Clause 247, page 199, line 14, after "extent" insert "within the United Kingdom"

299: Clause 247, page 199, line 17, after second "to" insert "the Isle of Man or"

300: Clause 247, page 199, line 18, at end insert—

"(6A) Any power under an Act to extend any provision of that Act by Order in Council to any of the Channel Islands may be exercised so as to extend there (with or without modifications) any amendment or repeal of that provision which is made by or under this Act."

Amendments 296 to 300 agreed.

Fit for Work Scheme

Question for Short Debate

7.36 pm

Asked by ***Lord Luce***

To ask Her Majesty's Government what progress has been made with the Fit for Work scheme in enabling those with long-term health problems like chronic pain to return to or stay in work.

Lord Young of Cookham (Con): My Lords, as this is now last business, the time limit has been extended to 90 minutes and the limit on individual speeches to 10 minutes.

Lord Luce (CB): My Lords, I am most grateful to the Minister for replying to this debate and to all noble Lords who will be offering their distinctive contributions. In July 2010 I led a short debate asking the Government what was being done to provide access to multidisciplinary pain management services in the NHS for those suffering chronic pain. Since then, the work of the Chronic Pain Policy Coalition and other specialist bodies has ensured progress, but it has been too slow.

I have suffered from chronic pain, caused by musculoskeletal problems, for more than 45 years. Thanks to prompt and effective support from private sector specialists in partnership with NHS doctors,

[LORD LUCE]

I have been fortunate enough to be able to perform a wide variety of public responsibilities. Many people with chronic pain do not have the same opportunity to find effective support to keep them in work. I want all who suffer to have sufficient support to enable them to stay in or return to work after absence through sickness.

The latest available research, published by the *British Medical Journal*, estimates that 8 million adults are living with chronic pain serious enough to prevent them from working or participating in normal everyday life. Moreover, the research estimated that over 40% of the population suffer chronic pain at some stage in their working lives which will affect their ability to work. This evidence makes it clear that it is not only the individual who suffers but society as a whole.

Society needs the maximum number of productive years from as many people as possible. The ratio of earners and wealth generators to dependants—children, pensioners, the unemployed—should be as high as possible, because those not working depend on those who are. Fortunately, people are living longer and retirement age is becoming more elastic. Individuals can contribute to the labour force for longer, so long as they are sufficiently well, mentally and physically, to work. I therefore welcome the Secretary of State's recent letter to me confirming that a Green Paper will be published before Christmas to consult on ways to ensure that government support meets the needs of people with health conditions in the workplace, and their employers.

It is shocking that the employment rate for adults with long-term conditions that affect their daily lives is only 46%, compared with 73% for the whole working-age population. The major long-term conditions include pain, musculoskeletal problems, stress and anxiety. Two major policy initiatives since 2008 have been the fit note and the Fit for Work service. Both are intended to enable sick individuals to return to work as soon as possible, with appropriate support. Early intervention is crucial to prevent a slide towards the benefits system. I know that the Minister is strongly committed to the Fit for Work service. I am giving him an opportunity to explain how it is developing and can be helped to succeed. Its effectiveness is something noble Lords will wish to probe.

Let me look briefly at the evolving history of sickness absence and its effect on society. In 2010, after 50 years of the sickness absence system, the Government replaced the sick note with a fit note. This was based on Dame Carol Black's report, *Working for a Healthier Tomorrow*. This note enabled GPs to focus for the first time on a patient's capacity to return to work, rather than their incapacity and the frequently repeated description "sick".

In 2011 came the publication of another report, *Health at Work—An Independent Review of Sickness Absence*, by Dame Carol Black and Mr David Frost. In 2013, the Government accepted their main recommendations: to establish a health and work advisory assessment unit and to introduce a Fit for Work service—government funded and designed to help workers with ill health. It includes an occupational health work-focused assessment for employees who are off sick, or likely to be so, for four weeks or more and an advice service for employees, employers and GPs. It is now fully rolled out so that GPs and employers throughout Britain can refer patients or employees to it. This service has the potential to fill a massive gap in current provision.

I want to take this opportunity to highlight my belief that this early intervention scheme is needed. Its success could bring enormous benefit to society, and some statistics will illustrate the point. Overall, working-age ill health costs the economy more than £100 billion, including lost productivity, sickness absence and other costs. The latest figure available on chronic back pain, from 2000, shows that it cost the economy £10 billion; it will therefore be far higher now. We also know that 900,000 people are absent through sickness for four weeks or more each year and that more than 25% of the working population have a long-term condition or impairment, particularly in the 40 to 55 age group. We know that more people want to work past pension age, which will inevitably mean many more with long-term health conditions at work. Chairing recently two Westminster Employment Forum seminars on this subject, my attention has also been drawn to something called presenteeism, where a large number of employees are not working to full capacity due to their lack of health and well-being.

All this means that society suffers. Employers face a loss of productivity; the nation spends considerable sums of taxpayers' money; and last but most important, the quality of life of many individuals is seriously undermined. Being out of work jeopardises any individual's self-esteem and morale. So I ask the Minister: what is working well, and how can the service made more effective?

A number of questions arise. GPs and other health professionals seem to lack awareness of this service, so is it publicised enough? Do GPs realise that their workload will be reduced by referring more patients to the occupational health service? Is there enough face-to-face contact for employees, in addition to the initial telephone advisory service? Do employees know that they can get help after four weeks off work by asking their GP or employer for a referral?

There are some successful examples of large companies helping affected employees. BT has helped some 30,000 people in the last eight years. I have heard that Anglian Water has achieved a return of £3 for every £1 spent in helping an employee and the Royal Mail a return of £5 for every £1, cutting absence by 25% over three years. But the Fit for Work service was intended to make occupational health advice available nationwide. This is difficult when, as I am told, there are only some 4,000 occupational health professionals, compared to more than 45,000 GPs and physiotherapists. What number of specialists are needed to provide a nationwide Fit for Work service? It would be helpful if the Minister could say something about progress on these matters, especially how the service is currently supporting small and medium-sized enterprises, which are less likely to be able to employ their own health specialists.

A major question arises: how well equipped is the NHS to give adequate professional support for those with long-term illnesses? I can speak only about chronic pain and musculoskeletal issues, while other noble Lords can no doubt speak of other areas. Patients

with chronic pain need to learn how to manage their pain and to know to what medical support they can turn—which may include physiotherapists, osteopaths, acupuncturists, psychologists and so on. A wide range of things can be done to keep us active and positive but many areas have inadequate or no multidisciplinary support for chronic pain. There is still a long way to go.

However, given an effective Fit for Work scheme, most suffering employees can be helped to stay in or return to work. Everyone stands to benefit: the individual, the employer and the nation. I congratulate the Minister on introducing this scheme. Would he be prepared for me to bring a small team from the Chronic Pain Policy Coalition and other interested Peers to discuss this scheme in more detail with him and, if possible, with Department of Health officials? I look forward to the Minister's response.

7.46 pm

Lord Fink (Con): My Lords, I thank the noble Lord, Lord Luce, for introducing the important topic of helping and enabling those with long-term health problems to return to or stay in work. I know that he identified chronic pain as a major category of health-related issues but those of us who have looked at some of the statistics know that mental health problems, as well as untreated drug and alcohol addictions, are also major causes of long-term health problems and unemployment. I believe that any effective initiatives that help society to deal with these problems are most laudable and I too congratulate the Minister on introducing these measures.

Traditionally, the first or only point of call for someone with such a health problem was the family GP. I know from direct experience how overworked our GP service is and while it usually does a good job in identifying and often in treating common health problems, particularly acute ones, its ability to help manage long-term chronic ones, particularly in the difficult areas of mental health, is rather more sorely tested—especially as a typical appointment with a doctor lasts less than 10 minutes.

As an employer, I also know how difficult it is to deal with employees who have chronic health problems that subsequently lead to extended time off work. Sadly, while many employers show compassion, some—particularly small businesses which have limited staff resources and important deadlines to work to—may focus more on the needs of the business than their employee's needs. Indeed, many small companies will not even have personnel departments to help them deal with the balance between showing the right compassion to the employee, respecting all of that employee's legal rights and the difficult job of meeting the business's needs.

As I understand it, while it is not a direct replacement of the traditional sick or fit note the Fit for Work initiative provides an integrated service, helping to improve health outcomes as well as employment outcomes by supporting both employees and employers. Given how much I believe that work is a great therapy that generates a sense of self-esteem, such esteem and purpose can help to offset many health problems such as depression. It can even take people's minds off pain. Indeed, long-term unemployment and depression can cause a vicious cycle, with negative effects on society in general and potentially devastating effects on the individual and his or her family. I look forward to hearing my noble friend the Minister describe the progress that the scheme has achieved.

7.50 pm

Baroness Thomas of Winchester (LD): My Lords, the noble Lord, Lord Luce, has done us all a service by highlighting this little-known scheme which was launched two years ago. The aim of the scheme is admirable and should help both the employee by facilitating a return to work and the employee's GP by preventing them having to write out yet more sick notes. At this point, I shall say how nice it is to have a different cast of characters speaking about DWP matters. I am sure the noble Lord agrees that it is very good when more people engage with DWP matters.

One only has to look at press comment about the scheme to see where some of the problems lie. When it was introduced, press headlines made it sound like a mandatory scheme, which it is not, to force sick employees back to work. I fear that a lot of damage has been done within the past decade by press comment ramping up the "shirkers and scroungers" mentality, thus tending to make those quite legitimately on sick benefits feel like frauds. The very title of this scheme—Fit for Work—sounds so like yet another assessment while a person is off sick that it is little wonder that some people may be getting the wrong end of the stick. Perhaps the scheme should be renamed and relaunched. I agree with the noble Lord, Lord Luce, that more positive and better publicity is certainly needed, not least because the number of referrals is well below what was expected.

The first problem is that the scheme is not known about nearly enough by employers and employees. The second problem is whether four weeks is too long an absence before a business can request help from the scheme. I gather that GPs can refer both earlier and later. Four weeks might be too long for employers, considering that the scheme is not mandatory. Perhaps there could be some flexibility.

Looking at the scheme itself, I understand it is to complement existing occupational health provision, where it exists, but we know that it exists only in large firms. We have heard about some of them. It will not exist in small businesses, where the bulk of employment lies. Small businesses are unlikely to know about the scheme. For that reason, I hope it will become much better known.

If the scheme is taken up, a telephone assessment will be undertaken by an occupational therapist—an OT—in the first instance who will prepare a return-to-work plan. Having taken advice from some OTs working in central London hospitals who have experience of treating those with long-term neuro or neuromuscular problems, I shall share their comments, which seem to me to be sensible and practical. The first thing they say is that OTs with a nursing or medical background often give general advice on what a person can or cannot do without giving more creative advice about how a person might adapt their usual way of going about things. In other words, a more specialised OT

[Baroness Thomas of Winchester]
might know from experience how to find a way around a difficulty. Perhaps specialised advice should be sought by some of the more general OTs.

My advisers also wonder what medical notes the Fit for Work scheme advisers have access to. If the answer is that they do not have access to such notes, then is an employee with complex needs going to be well served? Another problem is the telephone assessment. A lot of people do not like talking about confidential medical matters on the telephone. I know that face-to-face assessments are possible for those with complex conditions, but the travelling time to these assessments might be as much as 90 minutes. I wonder whether that will be having an impact on the take-up of this scheme and whether home visits are possible.

Then there is the problem of disclosure. A lot of employees, especially those with long-term conditions, will be very cautious about talking with a stranger about medical matters that might be shared with an employer. This last point is also one which is likely to apply to those with a mental health problem. The workplace mental health support service run by Remploy, which was set up to help those in work with a range of mild to moderate mental health problems, is slowly becoming more accessible and better known, and is, of course, part of access to work. Perhaps the Minister will tell us how this service fits into the scheme.

That brings me to the difficult question of the quality of assessors. My OT advisers are much too polite to make trenchant comments, but even they doubt whether there are enough well-trained, experienced OTs throughout the country to ensure enough consistency in assessments and advice. Are we spreading the available pool of OTs too thinly? Are more being trained for these and all the other assessments? If these problems I have mentioned could all be addressed, then I am sure the scheme would be much more successful.

As I have a minute more, I shall quickly make a point about chronic pain. It is a huge problem for a lot of people. It is reported to affect around 8 million adults. It is also reported that chronic back pain alone costs the country about £10 billion per annum. There is anecdotal evidence that the right degree of physical exercise can be beneficial. The noble Lord, Lord Luce, the Minister and I have talked before about the benefits of hydrotherapy for people with all kinds of severe musculoskeletal problems. Sadly, there is a terrible lack of hydrotherapy provision round the country, and hospital pools are closing for lack of money to maintain and staff them adequately. Considering that warm water exercise is beneficial for so many conditions, I wish the Government would give it their backing. I look forward to the Minister's reply.

7.57 pm

The Lord Bishop of Derby: My Lords, I, too, thank the noble Lord, Lord Luce, for introducing this debate with his characteristic mastery of the territory, context and issues.

I shall look at the progress of the Fit for Work scheme. As the noble Baroness, Lady Thomas, hinted, there has been a lot of negativity. I remember that when it was first introduced the press called it a test about whether people were fit for work. There have been pilots and a lot of chunter about the slow development of the rollout. We need to remember that it is a huge shift for the medical professional, employers and employees, and we need to encourage the Government to look carefully at the rollout to see what can be learned as it unfolds. As the noble Lord, Lord Fink, mentioned, there may be issues about how small businesses can access this opportunity.

I want to endorse the important potential of the scheme. Many of us know that when people fall out of work—and the problem is doubled, in a way, with ill-health factors—there are often issues with isolation, depression and not being in the social environment from which we human beings gather our identity and energy. When they feel excluded, people need to recognise that there is the possibility of inclusion in the future. That is why this scheme is so important and significant.

To try to draw that out, I shall offer an illustration from my work as a priest. I work with lots of individuals, including people with terrible, chronic, long-term pain and illness, and I also work in communities. I shall offer an analogy. We spend a lot of money in communities over many years and do not see many results. We pour it into outer estates, inner cities and needy groups, and 10 years later they want another round of grants and we wonder what has been achieved.

Noble Lords will know that there has been a recent move towards what is called "Asset Based Community Development". That means that if you try to develop a community by putting in things and adding value, you will discover what assets are already there in the people's gifts and in their interests, so that the people who live in a place or in a project own what is offered and imbibe it. It then becomes part of them and the whole thing involves people standing on their own feet and participating in the growth and development of their community.

The Fit for Work scheme could learn something from this, because there is a danger as the scheme unrolls—as the critics rightly say, it could be improved here and there—that we will develop an ever more sophisticated bureaucracy: we will tick that box, offer that service and make this available. But the whole point is to allow individuals who are suffering, and feeling isolated and possibly depressed, to own the possibility, with the scheme, of having their gifts and contribution recognised and to be given a platform, as the noble Lord, Lord Luce, said so eloquently, to participate in the world of work, in society and in business.

It would be very interesting if the Minister would reflect on this fact. As we learn from the pilots and the scheme is rolled out slowly and carefully, how can we enable the scheme, through the training of medical people and employers, to have the flexibility and the sensitivity to recognise that each person is an asset, as the noble Lord, Lord Luce, said? We should not just make them go through a scheme but enable them to feel, "I can participate in ways that suit my chronic pain"—or back injury or whatever it is—"and still make a contribution and still be included".

It is all about pace and timing. The danger of any scheme is that it gets its own bureaucracy and it rolls on. That is why community development so often does

not work. But if you can adjust the pace and the timing to allow creative participation from the individual concerned, the investment will be much more fruitful, there will be a much higher chance that people will get back into work in a strong way, and the scheme will flourish.

That is a massive ask of the Government and of those running the scheme: I recognise that. But I would invite the Minister to share his reflections on what we can learn from that asset-based approach, and on how the Government can ensure that those who administer the scheme can be as highly trained as possible to have that sensitivity and flexibility to allow the individual to be involved in the process and to be an asset in their own precious way so that they have dignity at work and a long-term future in it.

8.02 pm

Baroness Walmsley (LD): My Lords, I, too, congratulate the noble Lord, Lord Luce, on initiating this debate and I echo his call and that of other noble Lords for the benefits of the Fit for Work scheme to become more widely known. It really is mad that this great network of provision has been set up at great expense but that so many of the people who should know about it, especially GPs, do not make use of it.

I was so glad that my noble friend Lady Thomas of Winchester and the noble Lord, Lord Fink, both mentioned people with mental health problems. As the noble Lord said, they are often the primary cause of people being away from work for a long period, but I am sure we all know that many people who have chronic pain or another serious condition also have mental health problems that need to be addressed. I ask the Minister: what training do the occupational health advisers in the scheme have in identifying the mental health aspects of a person's absence from work and in signposting those people towards treatment that will help them overcome it?

I will concentrate my brief remarks on the issue of chronic pain. As we have heard, 8 million adults report chronic pain that is moderate to severely disabling, such that it prevents them working or living a normal life day to day. But many more people live with lesser levels of chronic pain. The incidence is, understandably, much higher in the older age groups. However, few of those people are likely to be in work and are therefore not affected by the Fit for Work programme that we are debating. However, it often prevents them volunteering in the way that they would like—and we all know how important older people are in that capacity. Most charities would fall apart without them.

In the working-age group, one of the conditions that produces chronic pain is fibromyalgia. I know something about this because a member of my family suffers from it. It is incurable and variable. She had such a level of pain and stiffness as to make it impossible for her to carry on with a job in the public service that she very much enjoyed. Eventually she was forced to take early retirement, which penalised her financially until she reached pensionable age. I know that her employer was very sorry to lose her, and I wonder whether she might have been able to carry on if the Fit for Work programme had been available at the time.

However, the rules of Fit for Work, as I understand them, are such that you are not eligible unless you have been, or are likely to be, absent from work for four weeks. I happen to know that my relative, although she suffered a lot of pain at work, did not have long periods of absence. But in the end, she found it just too difficult and retired early. I suspect that many people like her soldier on with a stiff upper lip, taking stronger and stronger painkillers, perhaps performing well below their capacity and not enjoying life at all. In many cases the employer, too, will suffer from their reduced productivity. I wonder whether more people could be helped if the scope of the programme were expanded to help people stay in work, rather than just to return to work from sick leave. Back pain is so common that I would be very surprised if there were not hundreds of thousands of people working below their full capacity because of it.

My family member worked in the public service and did not have an occupational health department to turn to. The Fit for Work programme fills that gap and is aimed at small and medium-sized businesses that often do not have the resources that are available to big corporates. But the point must be made that public service workers often do not have that, either, because they are scattered in smaller units around the country.

Occupational health professionals can often identify the obstacles that prevent a person returning to work or working at full capacity, and can avert the need for them to leave their job. Indeed, I suspect that these professionals would have a lot more clout when negotiating with employers about reasonable adjustments that could be made than the employee herself or himself. It would seem sensible and desirable that, just as reasonable adjustments must be made for workers with a disability, employers should also be prepared to make reasonable adjustments to help people with chronic pain retain their job and help the employer retain an experienced worker.

I am afraid my remarks have gone somewhat wider than the Fit for Work programme, but I think what I am calling for would also achieve some of the Government's objectives in setting up the scheme—for example, helping workers, improving productivity and increasing the tax take. I wonder therefore whether the Minister can tell me what action the Government are taking to widen the net and provide more help to a broader group of workers who are living with chronic pain but who keep calm and carry on in the good old British fashion.

8.08 pm

Lord McKenzie of Luton (Lab): My Lords, this has been an informed but brief debate and we should be grateful to the noble Lord, Lord Luce, who rightly prompted us to seek an update on the Fit for Work scheme, which has now been under way for more than a year. The particular focus of the noble Lord—and of others—was on chronic pain, for the reasons he outlined. The noble Lord also, in common with a number of other contributors, made the point forcefully that the service is as yet not well known.

The service has a direct link to the work of Dame Carol Black, and in particular to the analysis that she undertook, together with David Frost, that looked at

[Lord McKenzie of Luton]
sickness absence in the UK. Its focus on the period when people first became vulnerable to disconnection from the labour market was an important development and a component of emerging strands of policy that spanned Governments. Introduction of the service followed a series of pilots between April and June 2010 which looked at different ways of supporting employees in ill health to stay in or return to work after a period of sickness absence. These pilots grew out of Dame Carol's review of the health of Britain's working-age population, which showed the staggering annual economic cost of ill health in working days lost and worklessness to be over £100 billion.

Over recent years, the understanding of the relationship between work and health has changed and indeed improved. We have moved away from the notion that it is always in the best interests of someone with a health condition to be absent from the workplace. Being in work is good for health, and worklessness leads to poorer health—including mental health, a point noted by the noble Lord, Lord Fink. Hence the need to promote the benefits of work to health for individuals, employers and healthcare professionals, a proposition most strongly advanced by Waddell and Burton.

However, there is a need to go further. Bringing the expertise of health professionals directly to bear in support of individuals who are off sick or in danger of being so is something which we support. This is what the Fit for Work service is seeking to do. It is an early intervention, involving a referral after four weeks of sickness—although the noble Baroness, Lady Walmsley, made an interesting point about the relevance of that—for an assessment from a GP or, if not, potentially from an employer. That assessment should lead to a return to work plan. So far, so good, but we need to take stock to see how it is all working out in practice. I have some questions, some of which overlap those presented by other noble Lords. In England the service is contracted to Health Management Ltd. Can the Minister say something about the qualifications of the individuals allowed to deliver these services? What range of qualifications does this cover and what review of quality is being undertaken?

It is understood that the contract is for five years, at an initial value of something like £132 million, although this may have been increased. Can the Minister say how many Fit for Work interventions it is expected this would cover, and can we have an update on how many referrals have been made to date? Can the Minister say what level of referrals was anticipated when the contract was entered into?

Press comment, as others have noted, has suggested there is some confusion about the interpretation over the referral guidelines, at least so far as GPs are concerned. Is the Minister aware of this and can he say what the problem is? A DWP study apparently suggested GPs are likely to refer some 36% of their eligible case load to the service, but referral rates in practice vary. Why is this? The process involves at least the first assessment being undertaken by phone rather than face to face, and the nature of the assessment is determined by the occupational health professional. How many assessments are undertaken face to face and how many by phone? It is understood that a re-referral cannot be made within 12 months of a previous one where a return to work plan has been agreed. What is the position where an assessment is under way? Is it an iterative process, with potentially several telephone calls and meetings until a return to work plan is agreed? What is the experience of eligible employees who refuse consent for a referral? What information does the service hold on the outcome of return to work plans, in particular on whether they lead to long-term, sustainable, positive outcomes? The right reverend Prelate the Bishop of Derby offered an interesting parallel with asset-based community development and the potential that offers the Fit for Work service.

The Question of the noble Lord, Lord Luce, specifically refers to long-term, chronic pain, but of course the service is also available to those with a mental health condition. Can the Minister give us an update on the levels of referral for such individuals? Are such assessments always undertaken on a face-to-face basis, at least initially? It has also been reported that the Fit for Work service is less well used by SMEs, a point that a number of noble Lords made. Is this the Government's understanding, and what amendments might be made to the service to address that?

The Fit for Work service notwithstanding, major challenges exist. As the Work Foundation report due to launch next week sets out, managing a long-term health condition while also working is a challenge. People who experience multiple long-term health conditions have poorer outcomes from a range of employment-related conditions, which is perhaps not surprising. The Work Foundation reports that one in three current employees has at least one long-term health condition and that 42% report that their health affects their work. This, together with the stigma of discrimination associated with poor health, is argued to be a major contributor to the gap in employment outcomes.

We know that mental illness has a substantial and highly detrimental impact on employment outcomes when it occurs on its own, but an even greater impact when it occurs alongside a physical health condition. Nevertheless, it seems clear that for many people with multiple, long-term health conditions, work is a positive part of their lives. The question is what the Fit for Work service contributes to helping them remain in work. More needs to be done, as noble Lords have said, to enhance awareness of what it can do.

8.16 pm

The Minister of State, Department for Work and Pensions (Lord Freud) (Con): My Lords, I too thank the noble Lord, Lord Luce, for introducing this debate. I have spent a lot of time trying to get the service in, and it is absolutely vital that we have this kind of support for people, to stop the inflow at a time you can do it. That is what this service is designed to do. I also acknowledge the noble Lord's concerns about employees who are facing long-term sickness absence. We debated it quite some time ago now, I think when the independent review of sickness absence report, led by Dame Carol Black, came out. I hope I will be able to answer the bulk of the many questions that noble Lords have asked me.

I start by giving a picture of how the workforce in Great Britain has been affected by long-term sickness absence, a set of figures that has been touched on. In 2015, 139 million days were lost to sickness absence, and the independent review in 2011 on this came out with a total cost figure of £9 billion in sick pay and associated costs, with the whole cost to the economy running at £15 billion. Many noble Lords here today will remember that a significant proportion of sickness absences result from musculoskeletal conditions such as back or knee pain. The other big factor is mental health conditions, such as stress, depression and anxiety. Clearly, the fact that we have an ageing workforce adds to the necessity of having really good services in place to help those affected by health conditions to go back to work or to remain in work. As people are now living longer and healthier lives, it is vital that occupational health services are accessible for such workers so that they can continue to live at a better, healthier standard. The noble Baroness, Lady Thomas, asked me how many occupational health practitioners we really need in this country. That is a difficult question for me to answer. I think the answer is probably more than we have, but I cannot help her much more than that.

I do not want everyone to think that we focus only on services to help older workers to stay in work; age and health are not necessarily related. Many businesses already understand the benefits of providing occupational health support to employees but, as several noble Lords have pointed out today, one of the major issues is with the SMEs that do not have access to such support or have very limited access to it. That was one of the key findings from Dame Carol Black in her review, where she pointed out that it was the lack of access here that was preventing employees from returning to work. That led us to the establishment of the Fit for Work service.

As the noble Lord, Lord McKenzie, pointed out, we started with a gradual rollout in December 2014. We have now rolled out nationwide, and we offer occupational health assessments for those suffering from long-term sickness absence. We also provide an advice service for employers, GPs and employees that is free to use for all. That means that whenever an employee is absent from work due to illness for four weeks or more, they can be referred to Fit for Work by either their GP or their employer. It is interesting that the figures for employers have been moving ahead of those for GPs. Those who are referred are allocated their own experienced case manager who will conduct an assessment with them that will take into account all the issues—health, work and social issues—that may be preventing the member of staff from returning to work. The employee will receive a return to work plan detailing the steps that he or she, their employer or their GP can take to help them to return to work sooner. Then, provided that the employee consents, the plan is also sent directly to their employer or GP.

I turn to the question asked by the noble Baroness, Lady Walmsley, and the noble Lord, Lord McKenzie, on the qualifications of the healthcare professionals. They are professionals who have an occupational health qualification or occupational health experience or who are able to demonstrate the experience and skills appropriate to working in an occupational health context. Health professionals must be registered with the relevant regulatory and/or professional body on the appropriate parts of its registers. Fit for Work has an accredited specialist in occupational medicine providing clinical supervision of the service, and provides appropriate supervision from more experienced professionals from whom they can seek advice.

Both the right reverend Prelate the Bishop of Derby and the noble Baroness, Lady Thomas, asked who the health professionals are. They come from a wide range of backgrounds. They will signpost to other services if appropriate. I hope they are creative; they can refer on to hydrotherapy, for example, and the noble Baroness knows that I am a believer in much colder water than she is.

Employees and employers can contact the advice service on any work and health matter, and that includes people who are still in work. Someone—I have forgotten who but I think it may have been the noble Baroness, Lady Walmsley—talked about the stiff upper lip. The service is available for those with a stiff upper lip who are struggling at work. They do not have to be off work in order to take that advice.

The referrals are an iterative process, as said by the noble Lord, Lord McKenzie. An initial assessment will be done and an initial return to work plan issued. Further assessments will take place if required—for example, if an individual does not return to work as expected—and the service will provide support for up to three months if required.

I can give some numbers for the scheme. From the figures from March 2015 until last month, we are just shy of 10,000; some 9,000-odd people have gone through. For commercial reasons I cannot disclose our expectation but I will not disguise that that is a lower level than we had hoped for at this stage, and clearly we are concerned to do something about that. One thing we will do is reflect some of that in the Green Paper that is due between "shortly" and "soon"—we have had many debates about what those two words actually mean.

Some noble Lords mentioned some of the parallel services to Fit for Work. Noble Lords will remember that we introduced a tax exemption of up to £500 a year per employee for medical treatments recommended by Fit for Work with an employer-arranged occupational health service, so that is designed to act as an extra incentive for employers to make use of Fit for Work.

The Access to Work scheme provides practical and financial support with the additional costs faced by individuals whose health or disability affects the way they do their job. The amount of help that an individual may receive from Access to Work will depend on their individual need and personal circumstances, but the figure is now up to a maximum of £41,400 a year of support. The Access to Work programme is delivered by Jobcentre Plus. The awards are usually made for a period of three years and are reviewed annually. In answer to the question from the noble Baroness, Lady Thomas, I can say that Fit for Work will signpost to Access to Work as necessary. This will be recorded on the return to work plan for both the employee and their employer.

We know there is a consensus here. I am always delighted when the noble Lord, Lord McKenzie, and I agree on some of these matters; that was not always

[LORD FREUD]
the case. This Government are committed to helping more people with mental health conditions to find and retain work, as well as testing how to improve both the well-being and the employment prospects of claimants with mental health conditions. There is investment of an extra £1.25 billion in mental health support and we have pledged over £40 million over the next three years on a range of voluntary pilots to test how best to support people with mental health conditions to gain and retain employment.

The real issue here is that we often simply do not know what works. This money is really important to find some of those answers. I assure noble Lords that no one in the world knows them, so it is very important that we find out how to do it.

Government cannot do this on our own: we need employers and healthcare professionals. We believe that for Fit for Work to be more successful, for more people to go through it, there needs to be a change in culture among GPs and employers, particularly SMEs. There have been marketing campaigns to the medical community and to employers' representative bodies. Through them, the providers of Fit for Work have been working to increase awareness of the service across Great Britain but clearly—this is a point made by several noble Lords—we have a deal more work to do to get the word out.

The noble Lord, Lord McKenzie, asked about evaluation. An evaluation strategy is in place for Fit for Work. It is being undertaken by an independent research organisation on behalf of the work and health unit. It will include feedback from employee users, GPs and employers. The initial satisfaction data we have received from independent performance monitoring is that the service has been welcomed by GPs, employers and employees.

The noble Baroness, Lady Thomas, asked: should we rename and relaunch? We are looking at this whole area—should we expand, what is its role?—in the Green Paper, so we will be able to return to that topic. On the key question that she asked about sharing information, most people are relaxed about sharing information with their GP or employer. About 30% of people do not want to share the information.

The noble Lord, Lord Luce, asked whether the telephone is the right method. It is speedy, cost-effective and works in many cases. In some cases, it is not appropriate, and we will conduct face-to-face assessments when necessary.

My noble friend asked how well-equipped the NHS is to give support. NHS England commissions specialised care for patients whose pain cannot be successfully controlled or is particularly complex to manage. NICE has published several clinical guidelines and produced a range of best practice guidance on pain management for specialised drugs and treatment, as well as specific conditions, including chronic pain.

Too many individuals are still prevented from participating in the labour market by health issues. We have established the cross-government work and health unit jointly with the Department of Health. That is designed to lead the drive to improve work and health outcomes for people by improving integration across the healthcare and employment services. That combination is the driving factor behind Fit for Work.

We know that many larger companies see the benefit of supporting their workforces through occupational health—around 80% of large companies do that—but that only one in 10 small companies do so. That is where the Fit for Work service is designed to fill the hole. As I said, we will be exploring this area further in the Green Paper.

Let me conclude by again expressing my thanks to the noble Lord, Lord Luce. This is a key programme for us. It has not gone as rapidly as I hoped. I hope that, if we can get it up successfully and get the message out better, the benefits will be compelling: for employers, to reduce sick pay and increase productivity; for the state, as the noble Baroness, Lady Walmsley, said, through reduced long-term worklessness; but, most importantly, for the people involved, it just makes their lives more meaningful.

We are committed to doing everything we can to ensure that Fit for Work plays as full a part as possible in what is an extraordinarily important objective of helping people stay in work.

House adjourned at 8.35 pm.