

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION BILL [*LORDS*]

Eighth Sitting

Thursday 22 March 2018

(Afternoon)

CONTENTS

New clauses considered.
Bill, as amended, to be reported.

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

not later than

Monday 26 March 2018

© Parliamentary Copyright House of Commons 2018

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chairs: DAVID HANSON, †MR GARY STREETER

- | | |
|--|--|
| † Adams, Nigel (<i>Lord Commissioner of Her Majesty's Treasury</i>) | † Jones, Darren (<i>Bristol North West</i>) (Lab) |
| † Atkins, Victoria (<i>Parliamentary Under-Secretary of State for the Home Department</i>) | † Lopez, Julia (<i>Hornchurch and Upminster</i>) (Con) |
| † Byrne, Liam (<i>Birmingham, Hodge Hill</i>) (Lab) | † McDonald, Stuart C. (<i>Cumbernauld, Kilsyth and Kirkintilloch East</i>) (SNP) |
| † Clark, Colin (<i>Gordon</i>) (Con) | Murray, Ian (<i>Edinburgh South</i>) (Lab) |
| † Elmore, Chris (<i>Ogmore</i>) (Lab) | † O'Hara, Brendan (<i>Argyll and Bute</i>) (SNP) |
| Haigh, Louise (<i>Sheffield, Heeley</i>) (Lab) | † Snell, Gareth (<i>Stoke-on-Trent Central</i>) (Lab/Co-op) |
| † Heaton-Jones, Peter (<i>North Devon</i>) (Con) | † Warman, Matt (<i>Boston and Skegness</i>) (Con) |
| † Huddleston, Nigel (<i>Mid Worcestershire</i>) (Con) | † Wood, Mike (<i>Dudley South</i>) (Con) |
| † Jack, Mr Alister (<i>Dumfries and Galloway</i>) (Con) | † Zeichner, Daniel (<i>Cambridge</i>) (Lab) |
| † James, Margot (<i>Minister of State, Department for Digital, Culture, Media and Sport</i>) | Kenneth Fox, <i>Committee Clerk</i> |
| | † attended the Committee |

Public Bill Committee

Thursday 22 March 2018

(Afternoon)

[MR GARY STREETER *in the Chair*]

Data Protection Bill [Lords]

New Clause 7

APPLICATION OF EQUALITY ACT (SERVICES AND PUBLIC FUNCTIONS)

“(1) Part 3 (Services and public functions) of the Equality Act 2010 (‘the Equality Act’) shall apply to the processing of personal data by an algorithm or automated system in making or supporting a decision under this section.

(2) A ‘decision’ in this section means a decision or any part of a decision that engages a data subject (D)’s rights, freedoms or legitimate interests concerning—

- (a) the provision of services to the public and
- (b) the exercise of public functions by a service-provider.

(3) Nothing in this section detracts from other rights, freedoms or legitimate interests in this Act, the Equality Act or in any other primary or secondary legislation relating to D’s personal data, employment, social security or social protection.”—(*Liam Byrne.*)

This new clause would apply Part 3 of the Equality Act 2010 to the processing of personal data by an algorithm or automated system or supporting a decision under this new clause.

Brought up, and read the First time.

2 pm

Liam Byrne (Birmingham, Hodge Hill) (Lab): I beg to move, That the clause be read a Second time.

The Chair: With this it will be convenient to discuss the following:

New clause 8—*Application of the Equality Act (Employment)*—

“(1) Part 5 (Employment) of the Equality Act (‘the Equality Act’) shall apply to the processing of personal data by an algorithm or automated system in making or supporting a decision under this section.

(2) A ‘decision’ in this section means a decision that engages a data subject (D)’s rights, freedoms or legitimate interests concerning—

- (a) recruitment,
- (b) the terms and conditions of employment,
- (c) access to opportunities for promotion, transfer or training, and
- (d) dismissal.

(3) Nothing in this section detracts from other rights, freedoms or legitimate interests in this Act, the Equality Act or in any other primary or secondary legislation relating to D’s personal data, employment, social security or social protection.”

This new clause would apply Part 5 of the Equality Act 2010 to the processing of personal data by an algorithm or automated system or supporting a decision under this new clause.

New clause 9—*Right to algorithmic fairness at work*—

“(1) A person (“P”) has the right to fair treatment in the processing of personal data by an algorithm or automated system in making a decision under this section.

(2) A “decision” in this section means a decision in which an algorithm or automated system is deployed to support or make a decision or any part of that decision that engages P’s rights, freedoms or legitimate interests concerning—

- (a) recruitment,
- (b) the terms and conditions of employment,
- (c) access to opportunities for promotion, transfer or training, and
- (d) dismissal.

(3) “Fair treatment” in this section means equal treatment between P and other data subjects relevant to the decision made under subsection (2) insofar as that is reasonably practicable with regard to the purpose for which the algorithm or automated system was designed or applied.

(4) In determining whether treatment of P is “fair” under this section the following factors shall be taken into account—

- (e) the application of rights and duties under equality and other legislation in relation to any protected characteristics or trade union membership and activities,
- (f) whether the algorithm or automated system has been designed and trained with due regard to equality of outcome,
- (g) the extent to which the decision is automated,
- (h) the factors and weighting of factors taken into account in determining the decision,
- (i) whether consent has been sought for the obtaining, recording, using or disclosing of any personal data including data gathered through the use of social media, and
- (j) any guidance issued by the Centre for Data Ethics and Innovation.

(5) “Protected characteristics” in this section shall be the protected characteristics defined in section 4 of the Equality Act 2010.”

This new clause would create a right to fair treatment in the processing of personal data by an algorithm or automated system in making a decision regarding recruitment, terms and conditions of employment, access to opportunities for promotion etc. and dismissal.

New clause 10—*Employer’s duty to undertake an Algorithmic Impact Assessment*—

“(1) An employer, prospective employer or agent must undertake an assessment to review the impact of deploying the algorithm or automated system in making a decision to which subsection (1) of section [Application of Equality Act (Employment)] applies [an ‘Algorithmic Impact Assessment’].

(2) The assessment undertaken under subsection (1) must—

- (a) identify the purpose for which the algorithm or automated system was designed or applied,
- (b) test for potential discrimination or other bias by the algorithm or automated system,
- (c) consider measures to advance fair treatment of data subjects relevant to the decision, and
- (d) take into account any tools for Algorithmic Impact Assessment published by the Centre for Data Ethics and Innovation.”

This new clause would impose a duty upon employers to undertake an Algorithmic Impact Assessment.

New clause 11—*Right to an explanation*—

“(1) A person (“P”) may request and is entitled to be provided with a written statement from an employer, prospective employer or agent giving the following particulars of a decision to which subsection (1) of section [Right to algorithmic fairness at work] applies—

- (a) any procedure for determining the decision,
- (b) the purpose and remit of the algorithm or automated system deployed in making the decision,
- (c) the criteria or other meaningful information about the logic involved in determining the decision, and
- (d) the factors and weighting of factors taken into account in determining the decision.

(2) P is entitled to a written statement within 14 days of a request made under subsection (1).

(3) A complaint may be presented to an employment tribunal on the grounds that—

- (a) a person or body has unreasonably failed to provide a written statement under subsection (1),
- (b) the particulars given in purported compliance with subsection (1) are inadequate,
- (c) an employer or agent has failed to comply with its duties under section [Employer's duty to undertake an Algorithmic Impact Assessment],
- (d) P has not been treated fairly under section [Right to algorithmic fairness at work].

(4) Where an employment tribunal finds a complaint under this section well-founded the tribunal may—

- (e) make a declaration giving particulars of unfair treatment,
- (f) make a declaration giving particulars of any failure to comply with duties under section [Employer's duty to undertake an Algorithmic Impact Assessment] or section [Right to algorithmic fairness at work],
- (g) make a declaration as to the measures that ought to have been undertaken or considered so as to comply with the requirements of subsection (1) or section [Employer's duty to undertake an Algorithmic Impact Assessment] or section [Right to algorithmic fairness at work],
- (h) make an award of compensation as may be just and equitable.

(5) An employment tribunal shall not consider a complaint presented under subsection (3) in a case where the decision to which the reference relates was made—

- (i) before the end of the period of 3 months, or
- (j) within such further period as the employment tribunal considers reasonable in a case where it is satisfied that it was not reasonably practicable for the application to be made before the end of that period of 3 months.

(6) Nothing in this section detracts from other rights, freedoms or legitimate interests in this Bill or any other primary or secondary legislation relating to P's personal data, employment, social security or social protection."

This new clause would create a right to an explanation in writing from an employer, prospective employer or agent giving the particulars of a decision to which the Right to algorithmic fairness at work applies.

Liam Byrne: New clauses 7 and 8 to 11 touch on the question of how we ensure a degree of justice when it comes to decisions that are taken about us automatically. The growth in decisions that are made through automated decision making has been exponential, and there are risks to that. We need to ensure that the law is modernised to provide new protections and safeguards for our constituents in this new world.

I should say at the outset that this group of new clauses is rooted in the excellent work of the Future of Work commission, which produced a long, thought-provoking report. The Committee will be frustrated to hear that I am not going to read through that this afternoon, but, none the less, I want to tease out a couple of points.

The basket of new clauses that we have proposed are well thought through and have been carefully crafted. I put on record my thanks to Helen Mountfield QC, an expert in equality law, and to Mike Osborne, professor of machine learning. Along with Ben Jaffey QC, a specialist in data law, they have been looking at some of the implications of automated decision making, which were discussed at length by the Future of Work commission.

Central to the new clauses is a concern that unaccountable and highly sophisticated automated or semi-automated systems are now making decisions that bear on fundamental elements of people's work, including recruitment, pay and discipline. Just today, I was hearing about the work practices at the large Amazon warehouse up in Dundee, I think, where there is in effect digital casualisation. Employees are not put on zero-hours contracts, but they are put on four-hour contracts. They are guided around this gigantic warehouse by some kind of satnav technology on a mobile phone, but the device that guides them around the warehouse is also a device that tracks how long it takes them to put together a basket.

That information is then arranged in a nice league table of employees of who is the fastest and who is slowest, and decisions are then taken about who gets an extension to their contracted hours each week and who does not. That is a pretty automated kind of decision. My hon. Friend the Member for Eltham (Clive Efford) was describing to me the phenomenon of the butty man—the individual who decided who on a particular day got to work on the docks or on the construction site. In the pub at the end of the week, he divvied up the earnings and decided who got what, and who got work the following week. That kind of casualisation is now being reinvented in a digital era and is something that all of us ought to be incredibly concerned about.

What happens with these algorithms is called, in the jargon, socio-technical—what results is a mixture of conventional software, human judgment and statistical models. The issue is that very often the decisions that are made are not transparent, and are certainly not open to challenge. They are now quite commonly used by employers and prospective employers, and their agents, who are able to analyse very large datasets and can then deploy artificial intelligence and machine learning to make inferences about a person. Quite apart from the ongoing debates about how we define a worker and how we define employment—the subject of a very excellent report by my old friend Matthew Taylor, now at the RSA—there are real questions about how we introduce new safeguards for workers in this country.

I want to highlight the challenge with a couple of examples. Recent evidence has revealed how many recruiters use—surprise, surprise—Facebook to seek candidates in ways that routinely discriminate against older workers by targeting advertisements for jobs in a particular way. Slater and Gordon, which is a firm of excellent employment lawyers, showed that about one in five company executives admit to unlawful discrimination when advertising jobs online. The challenge is that when jobs are advertised in a targeted way, by definition they are not open to applicants from all walks of life, because lots of people just will not see the ads.

Women and those over the age of 50 are now most likely to be prevented from seeing an advert. Some 32% of company executives say that they have discriminated against those who are over 50, and a quarter have discriminated in that way against women. Nearly two thirds of executives with access to a profiling tool have said that they use it to actively seek out people based on criteria as diverse as age, gender and race. If we are to deliver a truly meritocratic labour market, where the rights of us all to shoot for jobs and to develop our skills and capabilities are protected, some of those practices have to stop. If we are to stop them, the law needs to change, and it needs to change now.

This battery of new clauses sets out to do five basic things. First, they set out some enhancements and refinements to the Equality Act 2010, in a way that ensures that protection from discrimination is applied to new forms of decision making, especially when those decisions engage core rights, such as rights on recruitment, terms of work, or dismissal. Secondly, there is a new right to algorithmic fairness at work, to ensure equal treatment. Thirdly, there is the right to an explanation when a decision is taken in a way that affects core elements of work life, such as a decision to hire, fire or suspend someone. Fourthly, there is a new duty for employers to undertake an algorithmic impact assessment, and fifthly, there are new, realistic ways for individuals to enforce those rights in an employment tribunal. It is quite a broad-ranging set of reforms to a number of different parts of legislation.

Daniel Zeichner (Cambridge) (Lab): My right hon. Friend is making a powerful case. Does he agree that this is exactly the kind of thing we ought to have been discussing at the outset of the Bill? The elephant in the room is that the Bill seems to me, overall, to be looking backwards rather than forwards. It was developed to implement the general data protection regulation, which has been discussed over many years. We are seeing this week just how fast-moving the world is. These are the kind of ideas that should have been driving the Bill in the first place.

Liam Byrne: Exactly. My hon. Friend makes such a good point. The challenge with the way that Her Majesty's Government have approached the Bill is that they have taken a particular problem—that we are heading for the exit door of Europe, so we had better ensure that we get a data-sharing agreement in place, or it will be curtains for Britain's services exports—and said, "We'd better find a way of incorporating the GDPR into British law as quickly as possible." They should have thought imaginatively and creatively about how we strengthen our digital economy, and how we protect freedoms, liberties and protections in this new world, going back to first principles and thinking through the consequences. What we have is not quite a cut-and-paste job—I will not describe it in that way—but neither is it the sophisticated exercise in public law making that my hon. Friend describes as more virtuous.

I want to give the Committee a couple of examples of why this is so serious, as sometimes a scenario or two can help. Let us take an individual whom we will call "Mr A". He is a 56-year-old man applying for website development roles. Typically, if someone is applying for jobs in a particular sector, those jobs will be advertised online. In fact, many such roles are advertised only online, and they target users only in the age profile 26 to 35, through digital advertising or social media networks, whether that is Facebook, LinkedIn, or others. Because Mr A is not in the particular age bracket being targeted, he never sees the ad, as it will never pop up on his news feed, or on digital advertising aimed at him. He therefore does not apply for the role and does not know he is being excluded from applying for the role, all as a consequence of him being the wrong age. Since he is excluded from opportunities because of his age, he finds it much harder to find a role.

The Equality Act, which was passed with cross-party consensus, prohibits less favourable treatment because of age—direct discrimination—including in relation to recruitment practices, and protects individuals based on their age. The Act sets out a number of remedies for individuals who have been discriminated against in that way, but it is not clear how the Bill proposes to correct that sin. Injustices in the labour market are multiplying, and there is a cross-party consensus for a stronger defence of workers. In fact, the Member of Parliament for the town where I grew up, the right hon. Member for Harlow (Robert Halfon), has led the argument in favour of the Conservative party rechristening itself the Workers' party, and the Labour party was founded on a defence of labour rights, so I do not think this is an especially contentious matter. There is cross-party consensus about the need to stand up for workers' rights, particularly when wages are stagnating so dramatically.

We are therefore not divided on a point of principle, but the Opposition have an ambition to do something about this growing problem. The Bill could be corrected in a way that made a significant difference. There is not an argument about the rights that are already in place, because they are enshrined in the Equality Act, with which Members on both sides of the House agree. The challenge is that the law as it stands is deficient and cannot be applied readily or easily to automated decision making.

Gareth Snell (Stoke-on-Trent Central) (Lab/Co-op): My right hon. Friend is making a powerful case about the importance of the Equality Act in respect of the Bill, but may I offer him another example? He mentioned the Amazon warehouse where people are tracked at work. We know that agencies compile lists of their more productive workers, whom they then use in other work, and of their less productive workers. That seems like a form of digital blacklisting, and we all know about the problems with blacklisting in the construction industry in the 1980s. I suggest that the new clauses are a great way of combating that new digital blacklisting.

Liam Byrne: My hon. Friend gives a brilliant example. The point is that employment agencies play an incredibly important role in providing workers for particular sectors of the economy, from hotels to logistics, distribution and construction. The challenge is that the areas of the economy that have created the most jobs in the 10 years since the financial crash are those where terms and conditions are poorest, casualisation is highest and wages are lowest—and they are the areas where productivity is poorest, too. The Government could take a different kind of labour market approach that enhanced productivity and wages, and shut down some of the bad practices and casualisation that are creating a problem.

As it happens, the Government have signed up to some pretty big ambitions in that area. Countries around the world recently signed up to the UN sustainable development goals. Goal 8 commits the Government to reducing inequality, and SDG 10 commits them to reducing regional inequality. However, when I asked the Prime Minister what she was doing about that, my question was referred to Her Majesty's Treasury and the answer that came back from the Chancellor was, "We believe in raising productivity and growth." The way to raise productivity and growth is to ensure that

there are good practices in the labour market, because it is poor labour market productivity that is holding us back as a country.

If digital blacklisting or casualisation were to spread throughout the labour market in the sectors that happen to be creating jobs, there would be no increase in productivity and the Government would be embarked on a self-defeating economic policy. Although these new clauses may sound technical, they have a bearing on a much more important plank of the Government's economic development strategy.

Our arguments are based on principles that have widespread support on both sides of the House and they are economically wise. The consequences of the new clauses will be more than outweighed by the benefits they will deliver. I commend them to the Minister and I hope she will take them on board.

2.15 pm

Darren Jones (Bristol North West) (Lab): I want to add some further comments in support of the new clauses.

The Science and Technology Committee, one of the two Committees that I sit on, has had a detailed debate on algorithmic fairness. It is important to understand what the new clauses seek to do. There is a nervousness about regulating algorithms or making them completely transparent, because there are commercial sensitivities in the coding in respect of the way they are published or otherwise.

These new clauses seek to put the obligation on to the human beings who produce the algorithms to think about things such as equalities law to ensure that we do not hardcode biases into them, as my hon. Friend the Member for Cambridge said on Second Reading. It is important to understand how the new clauses apply to the inputs—what happens in the black box of the algorithm—and the outputs. The inputs to an algorithm are that a human codes and sets its rules, and that they put the data into it for it to make a decision.

The new clauses seek to say that the human must have a consistent and legal obligation to understand the equalities impacts of their coding and data entry into the black box of the algorithm to avoid biases coming out at the other end. As algorithms are increasingly used, that is an important technical distinction to understand, and it is why the new clauses are very sensible. On that basis, I hope the Government will support them.

The Chair: I call the Minister, whose birthday it is today.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): Thank you, Mr Streeter, and what a wonderful birthday present it is to be serving on the Committee.

It is a joy, actually, to be able to agree with the Opposition on the principle that equality applies not only to decisions made by human beings or with human input, but to decisions made solely by computers and algorithms. On that, we are very much agreed. The reason that we do not support the new clauses is that we believe that the Equality Act already protects workers

against direct or indirect discrimination by computer or algorithm-based decisions. As the right hon. Member for Birmingham, Hodge Hill rightly said, the Act was passed with cross-party consensus.

The Act is clear that in all cases, the employer is liable for the outcome of any of their actions, or those of their managers or supervisors, or those that are the result of a computer, algorithm or mechanical process. If, during a recruitment process, applications from people with names that suggest a particular ethnicity were rejected for that reason by an algorithm, the employer would be liable for race discrimination, whether or not they designed the algorithm with that intention in mind.

The right hon. Gentleman placed a great deal of emphasis on advertising and, again, we share his concerns that employers could seek to treat potential employees unfairly and unequally. The Equality and Human Rights Commission publishes guidance for employers to ensure that there is no discriminatory conduct and that fair and open access to employment opportunities is made clear in the way that employers advertise posts.

The same principle applies in the provision of services. An automated process that intentionally or unintentionally denies a service to someone because of a protected characteristic will lay the service provider open to a claim under the Act, subject to any exceptions.

Liam Byrne: I am grateful to the Minister for giving way, not least because it gives me the opportunity to wish her a happy birthday. Could she remind the Committee how many prosecutions there have been for discriminatory advertising because employers chose to target their adverts?

Victoria Atkins: If I may, I will write to the right hon. Gentleman with that precise number, but I know that the Equality and Human Rights Commission is very clear in its guidance that employers must act within the law. The law is very clear that there are to be no direct or indirect forms of discrimination.

The hon. Member for Cambridge raised the GDPR, and talked about looking forwards not backwards. Article 5(1)(a) requires processing of any kind to be fair and transparent. Recital 71 draws a link between ensuring that processing is fair and minimising discriminatory effects. Article 35 of the GDPR requires controllers to undertake data protection impact assessments for all high-risk activities, and article 36 requires a subset of those impact assessments to be sent to the Information Commissioner for consultation prior to the processing taking place. The GDPR also gives data subjects the tools to understand the way in which their data has been processed. Processing must be transparent, details of that processing must be provided to every data subject, whether or not the data was collected directly from them, and data subjects are entitled to a copy of the data held about them.

When automated decision-making is engaged there are yet more safeguards. Controllers must tell the data subject, at the point of collecting the data, whether they intend to make such decisions and, if they do, provide meaningful information about the logic involved, as well as the significance and the envisaged consequences for the data subject of such processing. Once a significant decision has been made, that must be communicated to

the data subject, and they must be given the opportunity to object to that decision so that it is re-taken by a human being.

We would say that the existing equality law and data protection law are remarkably technologically agnostic. Controllers cannot hide behind algorithms, but equally they should not be prevented from making use of them when they can do so in a sensible, fair and productive way.

Daniel Zeichner: Going back to the point raised by my right hon. Friend, I suspect that the number of cases will prove to be relatively low. The logic of what the Minister is saying would suggest that there is no algorithmic unfairness going on out there. I do not think that that is the case. What does she think?

Victoria Atkins: I would be guided by the view of the Equality and Human Rights Commission, which oversees conduct in this area. I have no doubt that the Information Commissioner and the Equality and Human Rights Commission are in regular contact. If they are not, I very much hope that this will ensure that they are.

We are clear in law that there cannot be such discrimination as has been discussed. We believe that the framework of the law is there, and that the Information Commissioner's Office and the Equality and Human Rights Commission, with their respective responsibilities, can help, advise and cajole, and, at times, enforce the law accordingly. I suspect that we will have some interesting times ahead of us with the release of the gender pay gap information. I will do a plug now, and say that any company employing more than 250 employees should abide by the law by 4 April. I look forward to reviewing the evidence from that exercise next month.

We are concerned that new clauses 7 and 8 are already dealt with in law, and that new clauses 9 to 11 would create an entirely new regulatory structure just for computer-assisted decision-making in the workplace, layered on top of the existing requirements of both employment and data protection law. We want the message to be clear to employers that there is no distinction between the types of decision-making. They are responsible for it, whether a human being was involved or not, and they must ensure that their decisions comply with the law.

Having explained our belief that the existing law meets the concerns raised by the right hon. Member for Birmingham, Hodge Hill, I hope he will withdraw the new clause.

Liam Byrne: I think it was in "Candide" that Voltaire introduced us to the word "Panglossian", and we have heard a rather elegant and Panglossian description of a perfect world in which all is fine in the labour market. I am much more sceptical than the Minister. I do not think the current law is sufficiently sharp, and I am concerned that the consequence of that will be injustice for our constituents.

The Minister raised a line of argument that it is important for us to consider. The ultimate test of whether the law is good enough must be what is actually happening out there in the labour market. I do not think it is good enough; she thinks it is fine. On the nub of the argument, a few more facts might be needed on both sides, so we

reserve the right to come back to the issue on Report. This has been a useful debate. I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

New Clause 13

REVIEW OF ELECTRONIC COMMERCE (EC DIRECTIVE) REGULATIONS

"(1) The Secretary of State shall lay before both Houses of Parliament a review of the application and operation of the Electronic Commerce (EC Directive) Regulations 2002 in relation to the processing of personal data.

(2) A review under subsection (1) shall be laid before Parliament by 31 January 2019."—(*Liam Byrne.*)

This new clause would order the Secretary of State to review the application and operation of the Electronic Commerce (EC Directive) Regulations 2002 in relation to the processing of data and lay that review before Parliament before 31 January 2019.

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

This is not normally my practice, but let me raise another area that is subject to a measure of cross-party consensus. There is widespread recognition that the e-commerce directive, which is used to regulate information services providers, is hopelessly out of date. It was agreed in around 2000. In effect, it allows information services providers to be treated as publishers rather than publishers. Since then, we have seen the growth of big tech and the new data giants that now dominate the digital economy, and they are misbehaving. Worse, they have become platforms for hate speech, social division and interference in democracy. It was intriguing to hear Mark Zuckerberg himself admit in the interview he gave yesterday that Facebook was indeed being used to try to corrupt elections. That is an extraordinary recognition by the head of one of the most important firms in the world.

The Secretary of State for Digital, Culture, Media and Sport reminded us as recently as this morning that as we come out of the European Union we will have a new opportunity to update the e-commerce directive. The House basically must put in place a new framework to regulate information services providers in a new way. A debate is raging among our neighbours about what steps we need to take to shut down the hate speech that is dividing communities, and we need to get into that debate quickly. Germany recently passed laws that require companies such as Facebook to take down hate speech in a very short time window or face fines of up to €10 million and Ireland has created a new regulator to provide a degree of oversight, so it is intriguing that we are falling behind some of our most important neighbours, who now lead this debate.

I began looking at this issue when I started researching new techniques in ISIS propaganda. In the excellent Scotland Yard counter-terrorism referral unit, I saw propaganda that was put together with the slickness of a pop video to incite people to commit the most heinous crimes, such as the one we commemorate today. Yet I think we all recognise that organisations such as Facebook and YouTube are simply not working quickly enough to take down that kind of material, which we simply do

not want people to see. I congratulate *The Times*, which has run a forensic campaign to shine a light on some of that bad practice. It is good finally to see advertisers such as Unilever beginning to deliver a tougher message to social media platforms that enough is enough.

We know we have to modernise those regulations. The commercial world and politicians on both sides are saying, “Enough is enough.” We all fear the consequences of things going wrong with respect to the destabilisation of democracy in America—but not just in America. We have seen it across the Baltics, in France, in Germany, across southern Europe and in eastern Europe. Among our NATO allies, we can see a vulnerability to our enemies using social media platforms to sow division.

2.30 pm

I was recently in NATO StratCom in Latvia, where I watched with horror as some of our soldiers, working with NATO colleagues, showed how Russia is trying to foment a race war in Britain. It is beginning to pick the messages from the two most divisive sides of an argument—on one side, how radical Islam is destabilising Europe; on the other, how a new generation of neo-Nazis is on the rise—and promote them. We have an unholy alliance of bad countries and bad companies coming together. We can sit on our hands or do something about it. I suggest we do something about it.

The new clause would set a deadline for Government proposals to modernise the e-commerce directive. We will have to have a debate and make a choice about how close we bring the obligations and the liabilities of social media firms to the regulations we have for newspapers. Despite the hopelessly weak regulatory regime that the Government are intent on delivering in this country, there is no way on earth that even an IPSO-regulated newspaper could get away with the kind of nonsense that we see on social media—the kind of hate speech and viciousness that, more often than not I might add, is directed at women rather than men.

The new clause urges the Government to get on with that and states that by 31 January 2019—a little under a year’s time—we would have not the final law or regulations, but a review and a set of proposals on how the e-commerce directive needed to be reformed.

To my friends in the technology industry—as a former technology entrepreneur, I have many—I often make the point that we did not have one factory Act during the 19th century; we had 17. As technology, the economy, and custom and practice in the workplace changed, we had to update and modernise the regulation in this country. Frankly, that is the journey we are now on.

The Secretary of State vividly and colourfully said in *The Times*, and in his podcast with Nick Robinson, which comes out tomorrow, that the wild west is over and a new order will descend. The new clause urges the Government to put some deeds behind those grand words.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): I agree with everything the right hon. Gentleman has said, except that I do not think the Bill is the place for his proposals. The e-commerce directive and the Electronic Commerce (EC Directive) Regulations 2002, which transpose it into UK law, regulate services that are

“normally provided for remuneration, at a distance, by means of electronic equipment...and at the individual request of a recipient of a service”.

Those services are known as information society services.

However, questions relating to the processing of personal data by information society services are excluded from the scope of the e-commerce directive and hence excluded from the scope of the 2002 regulations. That is because the processing of personal data is regulated by other instruments, including, from May, the GDPR. The review of the application and operation of the 2002 regulations solely in relation to the processing of personal data, as proposed by new clause 13, would therefore be a speedy review to undertake.

However, that does not address the substance of the right hon. Gentleman’s concern, which we have already discussed in a delegated legislation Committee earlier this month. As I said then, the Government are aware of his concern that the e-commerce directive, finalised in 2000, is now outdated, in particular with regard to its liability provisions.

Those provisions limit, in specified circumstances, the liability that service providers have for the content on their sites. That includes social media platforms where they act as hosts. Social media companies have made limited progress on a voluntary basis, removing some particularly harmful content quickly and, in recent years, consistently. However, as we have seen in the case of National Action and its abhorrent YouTube videos, and many other lower-profile cases, there is a long way to go. We do not rule out legislation.

The Government have made it clear through our digital charter that we are committed to making the UK the safest place to be online, as well as the best place to grow a digital business. As the Prime Minister has said, when we leave the EU we will be leaving the digital single market, including the e-commerce directive. That gives us an opportunity to make sure that we get matters corrected for the modern age: supporting innovation and growth, and the use of modern technology, but doing so in a way that commands the confidence of citizens, protects their rights and makes their rights as enforceable online as they currently are offline.

The UK will be leaving the digital single market, but we will continue to work closely with the EU on digital issues as we build up our existing strong relationship in the future economic partnership. We will work closely with a variety of partners in Europe and further afield. Alongside that, our internet safety strategy will tackle the removal of harmful but legal content. Through the introduction of a social media code of practice and annual transparency report, we will place companies under an obligation to respond quickly to user reports and to ensure that their moderation processes are fit for purpose, with statutory backing if required. We have demonstrated that in the example of the introduction of age verification for online pornography.

There is an important debate to be had on the e-commerce directive and on platform liability, and we are committed to working with others, including other countries, to understand how we can make the best of existing frameworks and definitions. Consideration of the Bill in Committee and on Report are not the right places for that wide debate to be had. For those reasons, I request that the right hon. Gentleman withdraw the clause.

Liam Byrne: I admire the Minister's concern and ambition for administrative tidiness. She reminds me of an old quote by Bevin, who said once, "If you are a purist, the place for you is not a Parliament; it is a monastery."

Margot James: A nunnery.

Liam Byrne: In the case of the Minister, a nunnery, although Bevin was less enlightened than the hon. Lady. Here is a Bill; here is a new clause; the new clause is within scope. The object of the new clause is to deliver a Government objective, yet it is rejected. That is hard logic to follow. We have had the tremendous assurance, however, that there will be nothing less than a code of practice, so these huge data giants will be shaking in their boots in California, when they wake up. They will be genuinely concerned and no doubt already planning how they can reform their ways and stop the malpractice that we have grown all too used to. I am afraid that these amount to a collection of warm words, when what the country needs is action. With that in mind, I will push the new clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 7, Noes 10.

Division No. 15]

AYES

Byrne, rh Liam	O'Hara, Brendan
Elmore, Chris	Snell, Gareth
Jones, Darren	
McDonald, Stuart C.	Zeichner, Daniel

NOES

Adams, Nigel	Jack, Mr Alister
Atkins, Victoria	James, Margot
Clark, Colin	Lopez, Julia
Heaton-Jones, Peter	Warman, Matt
Huddleston, Nigel	Wood, Mike

Question accordingly negatived.

New Clause 16

CODE ON PROCESSING PERSONAL DATA IN EDUCATION

"(1) The Commissioner must consult on, prepare and publish a code of practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services, which relates to the rights of data subjects, appropriate to their capacity and stage of education.

(2) Before preparing a code or amendments under this section the Commissioner must consult the Secretary of State and such other persons as the Commissioner considers appropriate as set out in Clause 124 (3).

(3) In preparing a code or amendments under this section, the Commissioner must have regard—

- (a) that children have different capacity independent of age, including pupils who may be in provision up to the age of 25, and
- (b) to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child, and United Nations Convention on the Rights of Persons with Disabilities.

(4) For the purposes of subsection (1), "the rights of data subjects" must include—

- (a) measures related to Articles 24(3) (responsibility of the controller), 25 (data protection by design and by default) and 32(3) (security of processing) of the GDPR;
- (b) safeguards and suitable measures with regard to Articles 22(2)(b) (automated individual decision-making, including profiling), Recital 71 (data subject rights on profiling as regard a child) and 23 (restrictions) of the GDPR;
- (c) the rights of data subjects to object to or restrict the processing of their personal data collected during their education, under Articles 8 (child's consent to Information Society Services), 21 (right to object to automated individual decision making, including profiling) and 18(2) (right to restriction of processing) of the GDPR;
- (d) where personal data are biometric or special categories of personal data as described in Article 9(1) of the GDPR, the code should set out obligations on the controller and processor to register processing of this category of data with the Commissioner where it concerns a child, or pupil in education; and
- (e) matters related to the understanding and exercising of rights relating to personal data and the provision of education services."—(*Liam Byrne.*)

This new clause would require the Information Commissioner to consult on, prepare and publish a code of practice on standards to be followed in relation to the collection, processing, publication and other dissemination of personal data concerning children and pupils in connection with the provision of education services.

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

This is another entirely sensible new clause, which I hope the Government will take on board, either at this stage or on Report. We rehearsed earlier in Committee the debate about the reality and challenges of the fact that our education providers are now collecting, managing and often losing significant amounts of very personal data relating to children.

Any of us who has children at school will know the joys of ParentPay, which means that schools are collecting biometric data on our children. We know that schools are keeping exam results and all kinds of records and evaluations about our children online. Given the complexity of the GDPR and some of the costs and questions around implementing it, the complexity of the education system means that we urgently need a code of practice that schools can draw on to help them get the GDPR right, and to help our educators in their task of keeping our children's data safer than it is today.

In my argument, I will draw on the excellent contribution made on Second Reading by my noble Friend, Lord Knight, who said:

"Schools routinely use commercial apps for things such as recording behaviour, profiling children, cashless payments, reporting" and so on. My noble Friend has long been an advocate of that kind of thing, but the point is that he knows, and the other place recognised, that the way school information systems operate means they are often cloud based and integrated into all sorts of other data systems. There will often be contracts in place with all sorts of education service providers, which will entail the transfer of data between, for example, a school and a third party. It could well be that that third party is based overseas. As my noble Friend said:

“Schools desperately need advice on GDPR compliance to allow them to comply with this Bill when it becomes law.”—[*Official Report, House of Lords*, 10 October 2017; Vol. 785, c. 185.]

Lord Storey rode in behind my noble Friend, saying that

“young people probably need more protection than at any other time in our recent history.”—[*Official Report, House of Lords*, 10 October 2017; Vol. 785, c. 170.]

That is not something that has been debated only by the other place. UNICEF recently published a working paper entitled “Privacy, protection of personal information and reputation rights” and said it was now

“evident that children’s privacy differs both in scope and application from adults’ privacy”

but that they experience more threats than any other group. The “Council of Europe Strategy for the Rights of the Child (2016-2021)” echoed the same sentiment and observed:

“Parents and teachers struggle to keep up with technological developments”.

I have a number of friends who are teachers and headteachers. They listen to me in horror when I explain that I am the shadow Minister for the Data Protection Bill, because they know this is looming and they are absolutely terrified of it. Why is that? Because they are good people and good educators; they go into teaching because they want to change the world and change children’s lives, and they recognise the new obligations that are coming, but they also recognise the realities of how their schools operate today. Those people know about the proliferation of data that they and their staff are collecting. They know about the dangers and risks of that data leaking—not least because most teachers I know who have some kind of pastoral care responsibility seem to spend half their time having to advise their children about what not to do with social media apps and what not to post. They are often drawn in to disputes that rage out of control on social media platforms such as Instagram.

Teachers are very alert to the dangers of this new world. They are doing a brilliant and innovative job of supporting children through it, but they are crying out now for good guidance to help them to implement the GDPR successfully.

2.45 pm

Gareth Snell: I echo my right hon. Friend’s points. My daughter is seven years old. I have an app on my phone that, at any time of the day, will tell me what she is doing at school. Her attendance, reward system, and school meal requirements are all recorded on it, and I can access it at any time. The school she goes to wants to keep a connection with parents, so that parents can interact comfortably. The new clause would go a long way towards allowing schools to keep that link, because the default position of schools, as I am sure my right hon. Friend would agree, is to protect children, even if that means not sharing information in the way that they would like to.

Liam Byrne: That sounds like a terrifying application; my hon. Friend’s daughter very much has my sympathies. He is absolutely right. Lord Knight made this point with such power in the other place. The technology is advancing so quickly, and schools know that if they can

monitor things in new, more forensic ways, that helps them to do their job of improving children’s education. However, it has costs and consequences too. I hope that Her Majesty’s Government will look sympathetically on the task of teachers, as they confront this 200-and-heaven-knows-what-page Bill.

Darren Jones (Bristol North West) (Lab): Does my right hon. Friend share my concerns that, in response to a number of written parliamentary questions that I tabled, it became clear that the Government gave access to the national pupil database, which is controlled by the Government, to commercial entities, including newspapers such as *The Daily Telegraph*?

Liam Byrne: Yes. My hon. Friend has done an extraordinary job of exposing that minor scandal. I am surprised that it has not had more attention in the House, but hopefully once the Bill has passed it is exactly the kind of behaviour that we can begin to police rather more effectively.

I am sure that Ministers will recognise that there is a need for this. No doubt their colleagues in the Department for Education are absolutely all over it. I was talking to a headteacher in the Minister’s own constituency recently—an excellent headteacher, in an excellent school, who is a personal friend. The horror with which headteachers regard the arrival of the GDPR is something to behold. Heaven knows, our school leaders and our teachers have enough to do. I call on Ministers to make their task, their lives, and their mission that bit easier by accepting the new clause.

Victoria Atkins: Our schools handle large volumes of sensitive data about the children they educate. Anyone who has any involvement with the education system, either personally through their families, on their mobile phone apps, or in a professional capacity as constituency MPs, is very conscious of the huge responsibilities that school leaders have in handling that data properly and well, and in accordance with the law. As data controllers in their own right, schools and other organisations in the education system will need to ensure that they have adequate data-handling policies in place to comply with their legal obligations under the new law.

Work is going on already. The Department for Education has a programme of advice and education for school-leaders, which covers everything from blogs, a guidance video, speaking engagements, and work to encourage system suppliers to be proactive in helping schools to become GDPR-compliant. Research is also being undertaken with parents about model privacy notices that will help schools to make parents and pupils more aware of the data about children used in the sector. The Department for Education is also shaping a toolkit that will bring together various pieces of guidance and best practice to address the specific needs of those who process education data. In parallel, the Information Commissioner has consulted on guidance specifically addressing issues about the fair and lawful processing of children’s data. Everyone is very alive to the issue of protecting children and their data.

At this point, the Government want to support the work that is ongoing—already taking place—and the provisions on guidance that are already in the Bill. Our

concern is that legislating for a code now could be seen as a reason for schools to wait and see, rather than continuing their preparations for the new law. But it may be that in due course the weight of argument swings in favour of a sector-specific code of practice. That can happen. It does not have to be in the Bill. It can happen because clause 128 provides that the Secretary of State may require the Information Commissioner to prepare additional codes of practice for the processing of personal data, and the commissioner can issue further guidance under her own steam, using her powers under article 57 of the GDPR, without needing any direction from the Secretary of State.

I hope that the ongoing work reassures the right hon. Gentleman and that he will withdraw the new clause at this stage.

Liam Byrne: I am reassured by that and I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

New Clause 17

PERSONAL DATA ETHICS ADVISORY BOARD AND ETHICS CODE OF PRACTICE

(1) The Secretary of State must appoint an independent Personal Data Ethics Advisory Board (“the board”).

(2) The board’s functions, in relation to the processing of personal data to which the GDPR and this Act applies, are—

- (a) to monitor further technical advances in the use and management of personal data and their implications for the rights of data subjects;
- (b) to monitor the protection of the individual and collective rights and interests of data subjects in relation to their personal data;
- (c) to ensure that trade-offs between the rights of data subjects and the use of management of personal data are made transparently, inclusively, and with accountability;
- (d) to seek out good practices and learn from successes and failures in the use and management of personal data;
- (e) to enhance the skills of data subjects and controllers in the use and management of personal data.

(3) The board must work with the Commissioner to prepare a data ethics code of practice for data controllers, which must—

- (a) include a duty of care on the data controller and the processor to the data subject;
- (b) provide best practice for data controllers and processors on measures, which in relation to the processing of personal data—
 - (i) reduce vulnerabilities and inequalities;
 - (ii) protect human rights;
 - (iii) increase the security of personal data; and
 - (iv) ensure that the access, use and sharing personal data is transparent, and the purposes of personal data processing are communicated clearly and accessibly to data subjects.

(4) The code must also include guidance in relation to the processing of personal data in the public interest and the substantial public interest.

(5) Where a data controller or processor does not follow the code under this section, the data controller or processor is subject to a fine to be determined by the Commissioner.

(6) The board must report annually to the Secretary of State.

(7) The report in subsection (6) may contain recommendations to the Secretary of State and the Commissioner relating to how they can improve the processing of personal data and the protection of data subjects’ rights by improving methods of—

- (a) monitoring and evaluating the use and management of personal data;
- (b) sharing best practice and setting standards for data controllers; and
- (c) clarifying and enforcing data protection rules.

(8) The Secretary of State must lay the report made under subsection (6) before both Houses of Parliament.

(9) The Secretary of State must, no later than one year after the day on which this Act receives Royal Assent, lay before both Houses of Parliament draft regulations in relation to the functions of the Personal Data Ethics Advisory Board as listed in subsections (2), (3), (4), (6) and (7) of this section.

(10) Regulations under this section are subject to the affirmative resolution procedure.—(*Darren Jones.*)

This new clause would establish a statutory basis for a Data Ethics Advisory Board.

Brought up, and read the First time.

Darren Jones: I beg to move, That the clause be read a Second time.

New clause 17 is in my name and that of my right hon. Friend the Member for Birmingham, Hodge Hill. I do not take it personally that my other hon. Friends have not signed up to it; that was probably my fault for not asking them to do so in advance.

The new clause would bring a statutory footing to the data and artificial intelligence ethics unit, which I am very pleased that the Government have now funded and established, through the spring statement, in the Minister’s Department. It comes off the back of conversations with the Information Commissioner in Select Committee about the differing roles of enforcing legislation and of having a public debate about what is right and wrong and what the boundaries are in this ever-changing space. The commissioner was very clear that we need to have that debate with the public, but that it is not for her to do it. The ICO is an enforcer of legislation. The commissioner has a lot on her plate and is challenged by her own resource as it is. She felt that the new unit in the Department would be a good place to have the debate about technology ethics, and I support that assertion.

With no disrespect to any colleagues, I do not think that the House of Commons, and perhaps even the Select Committees to a certain extent, necessarily has the time, energy or resource to get into the real detail of some of the technology ethics questions, nor to take them out to the public, who are the people we need to be having the debate with.

The new clause would therefore establish in law that monitoring, understanding and public debate obligation that I, the ICO and others agree ought to exist in the new data ethics unit, but make it clear that enforcement was reserved for the Information Commissioner. I tabled the new clause because, although I welcome the Government’s commitment to the data and AI ethics unit, I feel that there is potential for drift. The new clause would therefore put an anchor in the technology ethics requirement of the unit so that it understands and communicates the ethical issues and does not necessarily get sidetracked into other issues, although it may seek to do that on top of this anchor. However, I think this anchor needs to be placed.

Also, I recognise that the Minister and the Secretary of State supported the recommendation made previously under the Cameron Government and I welcome that,

but of course, with an advisory group within the Department, it may be a future Minister's whim that they no longer wish to be advised on these issues, or it may be the whim of the Treasury—with, potentially, budget cuts—that it no longer wishes to fund the people doing the work. I think that that is not good enough and that putting this provision in the Bill would give some security to the unit for the future.

I will refer to some of the comments made about the centre for data ethics and innovation, which I have been calling the data and AI ethics unit. When it was first discussed, in the autumn Budget of November 2017, the Chancellor of the Exchequer said that the unit would be established

“to enable and ensure safe, ethical and ground-breaking innovation in AI and data-driven technologies. This world-first advisory body will work with government, regulators and industry to lay the foundations for AI adoption”.

Although that is a positive message, it says to me that its job is to lay the foundations for AI adoption. I agree with that as an aim, but it does not mean that at its core is understanding and communicating the ethical challenges that we need to try to understand and legislate for.

I move on to some of the documents from the recruitment advertising for personnel to run the unit from January of this year, which said that the centre will be at the centre of plans to make the UK the best place in the world for AI businesses. Again, that is a positive statement, but one about AI business adoption in this country, not ethical requirements. It also said that the centre would advise on ethical and innovative uses of data-driven tech. Again, that is a positive statement, but I just do not think it is quite at the heart of understanding and communicating and having a debate about the ethics.

My concern is that while all this stuff is very positive, and I agree with the Government that we need to maintain our position as a world leader in artificial intelligence and that it is something we need to be very proud of—especially as we go through the regrettable process of leaving the European Union and the single market, we need to hold on to the strengths we have in the British economy—this week has shown that there is a need for an informed public debate on ethics. As no doubt all members of the Committee have read in my *New Statesman* article of today, one of the issues we have as the voice of our constituents in Parliament is that in order for our constituents to understand or take a view on what is right or wrong in this quickly developing space, we all need to understand it in the first place—to understand what is happening with our data and in the technology space, to understand what is being done with it and, having understood it, to then to take a view about it. The Cambridge Analytica scandal has been so newsworthy because the majority of people understandably had no idea that all this stuff was happening with their data. How we legislate for and set ethical frameworks must first come from a position of understanding.

That is why the new clause sets out that there should be an independent advisory board. The use of such boards is commonplace across Departments and I hope that would not be a contentious question. Subsection (2) talks about some of the things that that board should do. The Minister will note that the language I have used is quite careful in looking at how the board should monitor developments, monitor the protection of rights and look out for good practice. It does not

seek to step on the toes of the Information Commissioner or the powers of the Government, but merely to understand, educate and inform.

The new clause goes on to suggest that the new board would work with the commissioner to put together a code of practice for data controllers. A code of practice with a technology ethics basis is important because it says to every data controller, regardless of what they do or what type of work they do, that we require ethical boundaries to be set and understood in the culture of what we do with big data analytics in this country. In working with the commissioner, this board would add great value to the way that we work with people's personal data, by setting out that code of practice.

I hope that the new clause adds value to the work that the Minister's Department is already doing. My hope is that by adding it to the Bill—albeit that current Parliaments cannot of course bind their successors and it could be legislated away in the future—it gives a solid grounding to the concept that we take technology ethical issues seriously, that we seek to understand them properly, not as politicians or as busy civil servants, but as experts who can be out with our stakeholders understanding the public policy consequences, and that we seek to have a proper debate with the public, working with enforcers such as the ICO to set, in this wild west, the boundaries of what is and is not acceptable. I commend the new clause to the Committee and hope that the Government will support it.

Margot James: I thank the hon. Gentleman for raising this very important subject. He is absolutely right. Data analytics have the potential to transform whole sectors of society and the economy—law enforcement and healthcare to name but some. I agree with him that a public debate around the issues is required, and that is one of the reasons why the Government are creating the centre for data ethics and innovation, which he mentioned. The centre will advise the Government and regulators on how they can strengthen and improve the way that data and AI are governed, as well as supporting the innovative and ethical use of that data.

3 pm

The centre will look at issues relating to both personal and non-personal data. Lord Stevenson of Balmacara said in the other place that

“it has not been possible to find a form of words for the powers that would be used to set up this advisory board”—
the board is mentioned in the new clause—

“which would be sufficiently broad to give a proper basis for the ambitions that we all share for it.”—[*Official Report, House of Lords*, 10 January 2018; Vol. 788, c. 297.]

I feel that the new clause brings us back to the point that Lord Stevenson said was problematic.

We plan to consult on the centre in the summer, after the chair has been appointed; we anticipate that appointment will be made in May. We would very much welcome the input of the hon. Member for Bristol North West, who is very knowledgeable on this issue.

The new clause would extend the commissioner's remit far beyond the application of what is required of her as the UK's supervisory authority for data protection. Given the breadth of the code that is set out in the new clause, it would essentially require the commissioner to

become a regulator on a much more significant scale than at present, and it would also create an overlap with the Electoral Commission, which is a separate regulator.

Three is more here that we agree on than disagree on, but the centre for data ethics and innovation, which we are in the process of creating, will, I trust, be the answer to much of the issue raised by the hon. Gentleman in his new clause. I hope that he feels confident enough in that to withdraw it.

Darren Jones: I thank the Minister for her co-operative words and for the invitation to be part of this developing area of public policy. Having already plugged my *New Statesman* article, I will plug a part of it, which is the news that, having worked with some of the all-party parliamentary groups, I am pleased that we will launch a commission on technology ethics with one of the Minister's colleagues, whose constituency I cannot quite remember, I am afraid, so I cannot make reference to him. But he is excellent.

We look forward to working with industry, stakeholders and politicians on a cross-party basis, to get into the debate about technology ethics. I accept the Minister's warm words about co-operating on this issue positively, so that hopefully the outcomes of this commission can perhaps help to influence the work of the unit, or centre, and the Government's response to it.

I would like this new unit to be given a statutory basis, to show its importance. It is vital that it has clout across Government and across Departments, so that it is not just a positive thing when we have Ministers who are willing to take part in and listen to this debate and instead is something that will go on with successive Ministers, should the current Minister be promoted, and with future Governments, too. However, in return for the Minister's warm words of co-operation, I am happy not to press the new clause to a vote today.

Daniel Zeichner: Very briefly, I declare an interest as the chair of the all-party parliamentary group on data analytics. This is a subject, of course, that is very dear to our hearts. I will just say that there is a great deal of common ground on it. I commend my hon. Friend the Member for Bristol North West for trying to put it into the Bill, because I, too, think it needs to be put on a statutory basis. However, I will just draw attention to a lot of the very good work that has been done by a whole range of people in bringing forward the new structures.

I will just say again that in general I think we are heaping a huge amount of responsibility on the Information Commissioner; frankly, we are now almost inviting her to save the world. She and her office will need help. So an additional body, with resources, is required.

The Royal Society and the British Academy have done a lot of work on this issue over the last few years. I will conclude by referring back to a comment made by the hon. Member for Gordon, because it is worth saying that the Royal Society and the British Academy state in the conclusions of their report:

"It is essential to have a framework that engenders trust and confidence, to give entrepreneurs and decision-makers the confidence to act now, and to realise the potential of new applications in a way that reflects societal preferences."

That is exactly the kind of thing we are trying to achieve. This body is essential and it needs to be set up as quickly as possible.

Darren Jones: I beg to ask leave to withdraw the new clause.

Clause, by leave, withdrawn.

New Clause 20

AUTOMATED NUMBER PLATE RECOGNITION (No. 2)

"(1) Vehicle registration marks captured by automated number plate recognition systems are personal data.

(2) The Secretary of State shall issue a code of practice in connection with the operation by the police of automated number plate recognition systems.

(3) Any code of practice under subsection (1) shall conform to section 67 of the Police and Criminal Evidence Act 1984."—
(*Liam Byrne.*)

This new clause requires the Secretary of State to issue a code of practice in connection with the operation by the police of automated number plate recognition systems, vehicle registration marks captured by which are to be considered personal data in line with the opinion of the Information Commissioner.

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

I will touch on this new clause only very briefly, because I hope the Minister will put my mind at rest with a simple answer. For some time, there has been concern that the way in which data collected by the police through automatic number plate recognition technology is not adequately ordered, organised or policed by a code of practice. A code of practice is probably required to put the police well and truly within the boundaries of the Police and Criminal Evidence Act 1984, the Data Protection Act 1998 and the Bill.

With this new clause, we are basically asking the Secretary of State to issue a code of practice in connection with the operation by the police of ANPR systems under subsection (1), and we ask that it conform to section 67 of the Police and Criminal Evidence Act 1984. I hope the Minister will just say that a code of practice is on the way so we can safely withdraw the new clause.

Victoria Atkins: I hope Committee members have had the chance to see my response to the questions of the hon. Member for Sheffield, Heeley on Tuesday about ANPR, other aspects of surveillance and other types of law enforcement activity.

I assure the right hon. Member for Birmingham, Hodge Hill that ANPR data is personal data and is therefore caught by the provisions of the GDPR and the Bill. We recognise the need to ensure the use of ANPR is properly regulated. Indeed, ANPR systems are governed by not one but two existing codes of practice. The first is the code issued by the Information Commissioner, exercising her powers under section 51 of the Data Protection Act 1998. It is entitled "In the picture: A data protection code of practice for surveillance cameras and personal information", and was published in June 2017. It is clear that it covers ANPR. It also refers to data protection impact assessments, which we debated last week. It clearly states that where the police and others use or intend to use an ANPR system, it is important that they

“undertake a privacy impact assessment to justify its use and show that its introduction is proportionate and necessary.”

The second code is brought under section 29 of the Protection of Freedoms Act 2012, which required the Secretary of State to issue a code of practice containing guidance about surveillance camera systems. The “Surveillance camera code of practice”, published in June 2013, already covers the use of ANPR systems by the police and others. It sets out 12 guiding principles for system operators. Privacy is very much a part of that. The Protection of Freedoms Act established the office of the Surveillance Camera Commissioner, who has a number of statutory functions in relation to the code, including keeping its operation under review.

In addition, a published memorandum of understanding between the Surveillance Camera Commissioner and the Information Commissioner sets out how they will work together. We also have the general public law principles of the Human Rights Act 1998 and the European convention on human rights. I hope that the two codes I have outlined, the Protection of Freedoms Act and the Human Rights Act reassure the right hon. Gentleman, and that he will withdraw his new clause.

Liam Byrne: I am indeed mollified. I beg to ask leave to withdraw the clause.

Clause, by leave, withdrawn.

New Clause 21

TARGETED DISSEMINATION DISCLOSURE NOTICE FOR THIRD PARTIES AND OTHERS (No. 2)

“In Schedule 19B of the Political Parties, Elections and Referendums Act 2000 (Power to require disclosure), after paragraph 10 (documents in electronic form) insert—

10A (1) This paragraph applies to the following organisations and individuals—

- (a) a recognised third party (within the meaning of Part 6);
- (b) a permitted participant (within the meaning of Part 7);
- (c) a regulated donee (within the meaning of Schedule 7);
- (d) a regulated participant (within the meaning of Schedule 7A);
- (e) a candidate at an election (other than a local government election in Scotland);
- (f) the election agent for such a candidate;
- (g) an organisation or a person notified under subsection 2 of this section;
- (h) an organisation or individual formerly falling within any of paragraphs (a) to (g); or
- (i) the treasurer, director, or another officer of an organisation to which this paragraph applies, or has been at any time in the period of five years ending with the day on which the notice is given.

(2) The Commission may under this paragraph issue at any time a targeted dissemination disclosure notice, requiring disclosure of any settings used to disseminate material which it believes were intended to have the effect, or were likely to have the effect, of influencing public opinion in any part of the United Kingdom, ahead of a specific election or referendum, where the platform for dissemination allows for targeting based on demographic or other information about individuals, including information gathered by information society services.

(3) This power shall not be available in respect of registered parties or their officers, save where they separately and independently fall into one or more of categories (a) to (i) of sub-paragraph (1).

(4) A person or organisation to whom such a targeted dissemination disclosure notice is given shall comply with it within such time as is specified in the notice.”

This new clause would amend the Political Parties, Elections and Referendums Act 2000 to allow the Electoral Commission to require disclosure of settings used to disseminate material where the platform for dissemination allows for targeting based on demographic or other information about individuals.—(Liam Byrne.)

Brought up, and read the First time.

Liam Byrne: I beg to move, That the clause be read a Second time.

The Chair: With this it will be convenient to discuss new clause 22—*Election material: personal data gathered by information society services*—

“In section 143 of the Political Parties, Elections and Referendums Act 2000 (Details to appear on electoral material), leave out subsection (1)(b) and insert—

- (b) in the case of any other material, including material disseminated through the use of personal data gathered by information society services, any requirements falling to be complied with in relation to the material by virtue of regulations under subsection (6) are complied with.”

This new clause would amend the Political Parties, Elections and Referendums Act 2000 to ensure that “any other material” clearly can be read to include election material disseminated through the use of personal data gathered by information society services.

Liam Byrne: I am happy to end on a note of cross-party consensus. We agree that we need to modernise our hopelessly outdated election laws. The news a couple of hours ago that the Information Commissioner’s application for a search warrant at Cambridge Analytica has been deferred—suspended until tomorrow—underlines the fact that the laws we have today for investigating malpractice that may impinge on the health of our democracy are hopelessly inadequate. The Information Commissioner declared to the world—for some reason on live television on Monday—that she was seeking a warrant to get into Cambridge Analytica’s office. Five days later there is still no search warrant issued by a court. Indeed, the court has adjourned the case until tomorrow.

I suspect that Cambridge Analytica has now had quite enough notice to do whatever it likes to the evidence that the Information Commissioner sought. This basket of clauses seeks to insert common-sense provisions to update the law in a way that will ensure that the data protection regime we put in place safeguards the health and wellbeing of our democracy. We need those because of what we now know about allegedly bad companies such as Cambridge Analytica, and because of what we absolutely know about bad countries such as Russia. We have been slow to wake up to the reality that, since 2012, Russia has been operating a new generation of active measures that seek to divide and rule its enemies.

There is no legal definition of hybrid war, so there is no concept of just war when it comes to hybrid war. There is no Geneva convention for hybrid war that defines what is good and what is bad and what is legal and illegal, but most legal scholars agree that a definition

of hybrid war basically touches on a form of intervening against enemies in a way that is deniable and sometimes not traceable. It contains a basket of measures and includes the kind of tactics that we saw deployed in Crimea and Ukraine, which were of course perfected after the invasion of Georgia. We see it in the Baltics and now we see it not just in America but across western Europe as well.

Such a technique—a kind of warcraft of active measures—has a very long history in Russia. Major-General Kalugin, the KGB's highest ranking defector, once described the approach as the “heart and soul” of Soviet intelligence. The challenge today is that that philosophy was comprehensively updated by General Gerasimov, the Russian Army's chief of staff, and it came alongside a very different world view presented by President Putin after his re-election as President in 2012 and in his first state of the union address in 2013. It was in that address that President Putin attacked what he called a de-Christianised morally ambivalent west. He set out pretty categorically a foreign policy of contention rather than co-operation.

Since 2012, we have seen what is basically a history of tactical opportunism. A little bit unlike the Soviet era, what we now have are sometimes authorised groups, sometimes rogue groups, seeking openings where they can and putting in place disruptive measures. They are most dangerous when they target the messiness of digital democracy. Here we have a kind of perfection of what I have called in the past a dark social playbook—for example, hackers such as Cozy Bear or Fancy Bear attacked the Democratic National Committee during the American elections.

We also have a partnership with useful idiots such as WikiLeaks, an unholy alliance with what are politely called fake news sites such as Westmonster or indeed Russia Today or Breitbart, which spread hatred. We have a spillover into Twitter. Once a row is brewing on Twitter, we get troll farms such as the Internet Research Agency in St Petersburg kicking in. Half of the tweets about NATO in the Baltics are delivered by robo-trolls out of Russia. It is on an absolutely enormous scale. Once the row is cooking on Twitter, we get the import into Facebook groups. They are private groups and dark groups, and it is perfectly possible to switch on dark money behind those ads circulating the hate material to thousands and thousands if not millions.

We know that that was standard practice in the German and French elections. There is a risk—we do not know what the risk is because the Government will not launch an inquiry—that such activity was going on in the Brexit campaign. I anticipate that there will be more revelations about that this weekend. However, the challenge is that our election law is now hopelessly out of date.

3.15 pm

There is a ban on political advertising on television, which is well established under section 321(2) of the Communications Act 2003. However, although political advertising is banned on television, psychographically targeted ads on Facebook are perfectly legal. In fact, the Advertising Standards Authority, which has long resiled from setting itself up as a truth commission that regulates political advertising, does not patrol or regulate political advertising on television. That is not an issue

because there is no political advertising any on television, but there is a lot of it on social media platforms, where it basically goes unregulated.

In addition, we have no provisions to shut down material against hate speech, because the e-commerce directive is so out of date. The Electoral Commission has no power to pursue the foreign money coming in behind some of these dark social ads. When I pressed it on that, it was clear that it does not have the power to pursue things abroad. Ofcom, too, does not regulate the content of video on social media platforms. We therefore have a situation where none of the Electoral Commission, Ofcom and the ASA has the power needed to operate, police and regulate political advertising and political campaigns in the digital era. We learn today that the Information Commissioner does not even have the power to get a search warrant when she needs one to investigate bad behaviour when compelling evidence comes to light.

It is clear that the law is hopelessly outdated. I hope this is a subject on which we can agree. We are now at the receiving end of a new generation of active measures, which are one of the greatest threats to us since the emergence of al-Qaeda at the beginning of the century. We must redouble our defences, so the new clause would give the Electoral Commission the power to issue targeted disclosure notices that require those who seek to influence a political campaign to share with the world information about who is being targeted with what and—crucially—who is writing the cheques.

Margot James: I will be brief in answering some of the serious matters raised by the right hon. Gentleman. The Information Commissioner, as the data regulator, is investigating alleged abuses as part of a broader investigation into the use of personal data during political campaigns. I have said many times that the Bill will add significantly to the commissioner's powers to conduct investigations, and I have confirmed that we keep an open mind and are considering actively whether further powers are needed in addition to those set out in the Bill.

The Electoral Commission is the regulator of political funding and spending. The commission seeks to bring transparency to our electoral system by enforcing rules on who can fund and how money can be spent, but new clause 21 is about sending the commission into a whole new field: that of personal data regulation. That field is rightly occupied by the Information Commissioner. We can debate whether she needs more powers in the light of the current situation at Cambridge Analytica, and as I have said we are reviewing the Bill.

While the Electoral Commission already has the power to require the disclosure of documents in relation to investigations under its current remit, new clause 21 would provide the commission with new powers to require the disclosure of the settings used to disseminate material. However, understanding how personal data is processed is outside the commission's remit.

The right hon. Gentleman suggested that his amendment would help with transparency on who is seeking to influence elections, which is very much needed in the current climate. The Government take the security and integrity of democratic processes very seriously. It is absolutely unacceptable for any third country to interfere in our democratic elections or referendums.

On new clause 22, the rules on imprints in the Political Parties, Elections and Referendums Act 2000 are clear. The current rules apply to printed election material no matter how it is targeted. However, the Secretary of State has the power under section 143 to make regulations covering imprints on other types of material, including online material. New clause 22 would therefore not extend the type of online material covered by such regulations. We therefore believe the new clause is unnecessary. The law already includes printed election material disseminated through the use of personal data gathered by whatever means, and the Government will provide further clarity on extending those rules to online material in due course by consulting on making regulations under the power in section 143(6).

On that basis, I ask the right hon. Gentleman to withdraw his new clause.

Liam Byrne: That is a deeply disappointing answer. I was under the impression that the Secretary of State said in interviews today that he is open-minded about the UK version of the Honest Ads Act that we propose. That appears to be in some contrast to the answer that the Minister offered.

What this country has today is an Advertising Standards Authority that does not regulate political advertising; Ofcom, which does not regulate video when it is online; an Electoral Commission without the power to investigate digital campaigning; and an Information Commissioner who cannot get a search warrant. Worse, we have a Financial Conduct Authority that, because it does not have a data sharing gateway with the Electoral Commission, cannot share information about the financial background of companies that might have been laundering money going into political and referendum campaigns. The law is hopelessly inadequate. Through that great hole, our enemies are driving a coach and horses, which is having a huge impact on the health and wellbeing of our democracy.

That is not a day-to-day concern in Labour constituencies, but it is for the Conservative party. Voter Consultancy Ltd took out targeted dark social ads aimed at Conservative Members, accusing some of them of being Brexit mutineers when they had the temerity to vote for common sense in a vote on Brexit in this House. Voter Consultancy Ltd, for those who have not studied its financial records at Companies House, as I have, is a dormant company. It has no accounts filed. There is no cash flowing through the books. The question that provokes is: where does the money come from for the

dark social ads attacking Conservative Members? We do not know. It is a matter of public concern that we should.

The law is out of date and needs to be updated. I will not press the matter to a vote this afternoon because I hope to return to it on Report, but I hope that between now and then the Minister and the Secretary of State reflect on the argument and talk to Mark Sedwill, the National Security Adviser, about why the national security strategy does not include an explicit objective to defend the integrity of our democracy. I hope that that change is made and that, as a consequence, further amendments will be tabled to ensure that our democracy is protected against the threats we know are out there.

I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

Question proposed, That the Chair do report the Bill, as amended, to the House.

Margot James: On a point of order, Mr Streeter. I wanted to thank you, and Mr Hanson in his absence, as well as, in the House of Lords, my noble Friends Lord Ashton, Baroness Williams, Lord Keen, Baroness Chisholm and Lord Young, and the Opposition and Cross-Bench peers. I also thank the Under-Secretary of State for the Home Department, my hon. Friend the Member for Louth and Horncastle, and the Opposition Front Bench Members—the right hon. Member for Birmingham, Hodge Hill, with whom it has been a pleasure debating in the past two weeks, and the hon. Member for Sheffield, Heeley, who was not able to be in her place this afternoon.

I offer great thanks to both Whips. It was the first Bill Committee for my hon. Friend the Member for Selby and Ainsty in his capacity as Whip, and my first as Minister, and it has been a pleasure to work with him. I also thank the hon. Member for Ogmores. My hon. Friend the Under-Secretary and I are grateful to our Parliamentary Private Secretary, my hon. Friend the Member for Mid Worcestershire, who has worked terribly hard throughout the proceedings, as indeed have the Clerks, the *Hansard* writers, the Doorkeepers and the police. Without the officials of my Department and, indeed, the Home Office, we would all have been bereft, and I am most grateful to all the officials.

Question put and agreed to.

Bill, as amended, accordingly to be reported.

3.25 pm

Committee rose.

Written evidence reported to the House

DPB 50 Patrick Daly, Newspaper Conference

DPB 51 Index on Censorship, English PEN, Reporters Without Borders

DPB 52 Richard Parker, Senior Associate, Hill Dickinson LLP

DPB 53 Associated Newspapers

DPB 54 National Union of Journalists

DPB 55 Law Society of Scotland

DPB 56 Curtis Banks Group Plc

DPB 57 Foot Anstey LLP

DPB 58 Nikita Aggarwal

