LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on the Data Protection Bill 2017 for Committee Stage in the House of Lords

October 2017

About Liberty

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

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

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

Contact

Corey Stoughton
Advocacy Director
Direct Line 020 7378 3667
Email: coreys@liberty-human-rights.org.uk

Silkie Carlo
Senior Advocacy Officer
Direct Line 020 7378 5255
Email: silkiec@liberty-human-rights.org.uk

Gracie Mae Bradley
Advocacy and Policy Officer
Direct Line: 0207 378 3654
Email: gracieb@liberty-human-rights.org.uk

CONTENTS

INTRODUCTION

Liberty welcomes the opportunity to provide briefing and amendments to the Data Protection Bill 2017 for Committee Stage in the House of Lords.

This briefing sets out the following proposals:

- To **protect individuals from being subjected to significant automated decisions that engage their fundamental rights**
- To **maintain basic data rights to restrict and object to processing**, for example where data accuracy is contested, or the processing lacks a legitimate or lawful basis, in relation to overly broad purposes such as taxing, administering housing benefit, and the "maintenance of effective immigration control"
- To **maintain individuals' basic data rights where data is being processed for the "maintenance of effective immigration control"**, or "the investigation or detection of activities that would interfere with effective immigration control"
- To **remove excessively broad delegations** of law-making power to the Secretary of State

Exemptions on the right not to be subject to automated decision-making

Amendments

General automated processing

Clause 13, page 7, line 11, at end insert -

"(2A) A decision that engages an individual's rights under the Human Rights Act 1998 does not fall within Article 22(2)(b) of the GDPR (exception from prohibition on taking significant decisions based solely on automated processing for decisions that are authorised by law and subject to safeguards for the data subject's rights, freedoms and legitimate interests)."

Law enforcement automated processing

Clause 48, page 28, line 28, at end insert –

"( ) does not engage the rights of the data subject under the Human Rights Act 1998."

Intelligence services automated processing

Clause 94, page 54, line 26, insert after 'law' 'unless the decision engages an individual's rights under the Human Rights Act 1998'

Clause 94, page 54, line 29, leave out paragraph (c)

Clause 95, page 55, line 1, leave out paragraph (b) (*consequential to the amendment above)*

Delegated powers

Clause 13, page 7, line 40, leave out subsection (6)

Clause 13, page 7, line 40, leave out subsection (7)

Clause 48, page 29, line 4, leave out subsection (4)

Clause 48, page 29, line 9, leave out subsection (5)

Effect

These amendments would clarify that **the exemption from prohibition on taking significant decisions based solely on automated processing must not apply to purely automated decisions that engage an individual's human rights**. The amendment to Clause 13 applies to general processing; the amendment to Clause 48 applies to law enforcement processing; the amendment to Clause 94 applies to intelligence services processing.

The amendments to Clause 94(2)(c) and Clause 95(2)(b) would **remove the exemption** for intelligence agencies to automatically process personal data to make decisions significantly affecting a data subject **for the purpose of considering, entering or performing a contract**.

These amendments regarding delegated powers would **remove the powers delegated to the Secretary of State to amend the safeguards applying to automated decision-making** authorised by law. The amendments to Clause 13 apply to general processing; the amendments to Clause 48 apply to law enforcement processing.

Briefing

Under the Data Protection Act 1998, individuals have a qualified right not to be subject to purely automated decision making and, to the extent that automated decisions are permitted, a right to access information relating to automated decisions made about them.[1] The GDPR clarifies and extends these rights.

Article 22 of the GDPR gives individuals a right not to be subject to purely automated decision making:

> *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."*[2]

This right does not apply if the decision is authorised by EU or the Member State's law so long as the data subject's rights, freedoms and legitimate interests are safeguarded.[3] Liberty believes that the safeguarding of data subjects' rights and freedoms clearly includes their rights provided by the Human Rights Act 1998. These amendments would explicitly state

[1] Data Protection Act 1998, s.12
[2] GDPR, Article 22(1)
[3] GDPR, Article 22(2)(b)

that, therefore, automated decisions that engage an individual's human rights are not permissible.

This is an important safeguard of increasing relevance as automated decision-making, often based on big data aggregation or passive bulk surveillance, is of growing use.

General processing

In relation to general automated processing (clause 13), the explicit protection of human rights would protect individuals from being subjected to automated decisions that could engage their fundamental rights - for example, by unfairly discriminating against them. A recent study claimed that a facial recognition tool was able to 'detect' individuals' sexuality based on their photographs, taken from online dating sites, with greater accuracy than humans.[4] Another recent study claimed that a machine learning tool was able to diagnose depression by scanning individuals' photos posted on the social media platform Instagram with greater accuracy than the average doctor.[5] The rapidly growing field of machine learning and algorithmic decision making clearly presents new and very serious risks. As a minimum, individuals' basic rights must be explicitly protected at all times, and regarded as paramount.

Law enforcement processing

Law enforcement agencies are exempted from the prohibition on making purely automated, significant decisions (clause 47) – 'significant' decisions being those that significantly or adversely affect the data subject[6] - if the decision is required or authorised by law.[7] We believe such a decision should not be authorised by law if it engages an individuals' human rights, and the amendment we suggest to clause 48 would make this protection explicit.

Liberty is deeply concerned about the potential uses of purely automated decision-making in the law enforcement environment, particularly in relation to the 'significant' decisions that have adverse legal effects that are exempted here. We believe that automated processing, if used, should inform officers' decisions rather make those decisions. Controversial algorithms

[4] Deep neural networks are more accurate than humans at detecting sexual orientation from facial images (preprint) - Yilun Wang & Michal Kosinski, OSF, 15 Feb 2017
[5] Instagram photos reveal predictive markers of depression - Andrew G Reece & Christopher M Danforth, EPJ Data Science, 8 August 2017
[6] Data Protection Bill 2017, cl. 47(2)
[7] Data Protection Bill 2017, cl. 47(1) and cl. 48(1)(b)

currently being trialled by police forces, such as the harm assessment risk tool used in bail decisions and automated facial recognition that leads to arrests, are currently used to *support* officers' decisions. They do not replace officers' decisions or remove their discretion.[8] However, such purely automated decisions could be permitted under the exemptions within clauses 47 and 48.

Sophisticated algorithms used by law enforcement agencies such as the harm assessment tool and automated facial recognition are involved in decisions that engage fundamental rights such as the right to liberty, the right to a private life, freedom of expression, freedom of assembly and the prohibition of discrimination. The right not to be subjected to a purely automated decision – in other words, the requirement of human involvement in decision-making – is thus a vital safeguard, from which we do not believe law enforcement should be exempted.

We urge parliamentarians, as a very minimum, to amend the Bill to protect individuals from being subjected to significant automated decisions that engage their fundamental rights.

Intelligence services automated processing

Similarly, we are concerned that the Bill currently permits the intelligence services to make purely automated decisions that have significant effects, including legal effects, as regards an individual. This could create significant risks for the upholding of basic rights in relation to new and emerging technologies.

The amendment we have suggested to cl. 94(2) is a bare minimum protection that would still permit intelligence agencies to make purely automated decisions that have significant effects, including legal effects, where the decision is required or authorised by law – but that critically, would disallow decisions that engage an individual's rights under the Human Rights Act 1998 from being purely automated. This amendment would protect such basic rights as the right to liberty and the prohibition of discrimination from being engaged by solely automated means. In Liberty's view, human involvement in decision-making is a basic and vital safeguard for our fundamental rights, particularly as we traverse the technological revolution.

[8] For example: "*While HART forecasts support the custody officer's decision making, they quite explicitly do not remove the officer's discretion*" - written evidence submitted by Durham Constabulary (ALG0041; para. 7) in response to the Science and Technology Committee's inquiry into algorithms in decision making – April 2017: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69063.html

Clause 94(2)(c) creates a perplexing exemption from automated decision-making rights, unavailable to law enforcement or indeed private bodies, in relation to the consideration of contracts. We do not believe that the consideration of contracts justifies subjecting an individual to a purely automated decision, based on the processing of personal data, that has significant legal effects. Therefore, our suggested amendment to remove cl. 94(2)(c) and consequentially cl. 95 (2)(b) would help to assimilate data protections in the law enforcement and intelligence contexts by removing what appears to be a tenuous exemption from vital protections.

Exemptions from the right to restriction of processing

Amendment

Schedule 2, page 124, paragraph 1, line 17, leave out subparagraph (a)(vi)

Effect

This amendment would remove the exemption from data subjects' right to restrict the processing of their data (where data accuracy is contested, or the processing is unlawful, or the data is required for the exercise of a legal claim) in relation to a variety of broad purposes including the prevention and detection of crime, [9] tax purposes,[10] risk assessment systems including in the administering of housing benefit,[11] and the "maintenance of effective immigration control".[12]

Exemptions from the right to object

Amendment

Schedule 2, page 124, paragraph 1, line 19, leave out subparagraph (a)(viii)

Effect

This amendment would remove the exemption from data subjects' right to object to data processing (where there is an absence of compelling legitimate grounds) in relation to a variety of broad purposes including the prevention and detection of crime, [13] tax purposes,[14] risk assessment systems including in the administering of housing benefit,[15] and the "maintenance of effective immigration control".[16]

[9] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 2(1)(a)
[10] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 2(1)(c)
[11] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 3(2)(a)
[12] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(1)
[13] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 2(1)(a)
[14] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 2(1)(c)
[15] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 3(2)(a)
[16] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(1)

Exemptions on immigration control grounds

Amendment

Schedule 2, page 125, line 40, leave out paragraph 4.

Explanation

This amendment removes an exemption to data subjects' rights where personal data is being processed for the maintenance of effective immigration control, or for the investigation or detection of activities that would undermine it.

Briefing

The immigration control exemption creates a two-tier, discriminatory data protection regime

Schedule 2, paragraph 4 of the Bill, hereafter referred to as "the immigration control exemption," proposes to create a new exemption from individuals' data privacy rights when their data is processed for:

a) the maintenance of effective immigration control,[17] or
b) the investigation or detection of activities that would interfere with effective immigration control,[18]

to the extent that the fulfilment of their rights would prejudice these activities.

The inclusion of an immigration control exemption in the Bill is a brazen violation of the data protection and privacy rights of migrants – both documented and undocumented – and indeed, of their families and communities, in the name of immigration control. In effect, it removes all of the Home Office's data protection obligations as they relate to its activities to control immigration, as well as those of any other agency processing personal data for the same purpose, or sharing data with another agency processing it for that purpose.

The exemption would affect the rights listed at paragraph one of schedule 2,[19] and set out in full in the GDPR at Articles 13(1)-(3), 14(1)-(4), 15(1)-(3), 16, 17(1)-(2), 18(1), and 20(1)-(2). The exemption also covers the general principles set out in Article 5 as they apply to these rights. The exemption covers essentially all rights held by data subjects, including rights of

[17] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(1)(a)
[18] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 4(1)(b)
[19] Data Protection Bill 2017, Schedule 2, Part 1, paragraph 1(a)-(b)

subject access, rights of rectification and erasure, and the right to know who is processing data, which data, and for what purpose, including when that data has been obtained from a third party and not from the individual themselves.

Sub-paragraphs 2 and 3 of paragraph 4 exempt data controllers that process and share data with a second controller for the purposes of immigration control or investigation of activities that would undermine it from their obligations under GDPR Articles 13(1)-(3), 14(1)-(4), 15(1)-(3) and Article 5, to the extent that the second controller is also exempt from the generally applicable safeguards contained in those GDPR provisions.

Lord Ashton of Hyde has stated that under section 19(1)(a) of the Human Rights Act 1998, in his view, the Bill's provisions are compatible with the rights contained in the European Convention on Human Rights (ECHR). However, this immigration control exemption, insofar as it establishes an inferior data protection regime for those whose data is processed on immigration control grounds, is clearly indirectly discriminatory on the grounds of nationality and incompatible with Articles 8 and 14 of the Convention. It is deeply concerning that the Home Office and other data controllers processing information for immigration control purposes would be untethered from foundational principles such as lawfulness, fairness, transparency or accountability as set out in Article 5 of the GDPR in their use of data to make immigration-related decisions that may have an irreversible impact on an individual's life, or to refuse them access to essential public services on the grounds of their immigration status.

This is not the first time that Government has attempted to limit data protection rights on immigration control grounds. Clause 28 of the 1983 Data Protection Bill had an identical aim, setting out broad exemptions to data subjects' rights on grounds of crime, national security and immigration control. The Data Protection Committee, then chaired by Sir Norman Lindop, said that the clause would be "a palpable fraud upon the public if [it] were allowed to become law"[20] because it allowed data acquired for one purpose to be processed for another.

In the House of Lords, Lord Avebury raised concerns almost synonymous with those that we raise today, namely that:

[20] Lord Elystan-Morgan, Data Protection Bill [H.L.] HL Deb 21 July 1983 vol 443 cc1269-311http://hansard.millbanksystems.com/lords/1983/jul/21/data-protection-bill-hl#S5LV0443P0_19830721_HOL_172

> "the provision is in danger of being oppressive, deeply worrying to the immigrant community living among us, and one which is in grave danger of infringing the provisions of the [European Convention on Human Rights]."[21]

Clause 28 was rightfully removed from the 1983 Bill. However, we see it resurrected today in even more startling breadth as paragraph 4 of Schedule 2. As it was called upon to do 35 years ago, the House of Lords should reject this unwise, unfair and unprecedented exemption.

- The immigration control exemption risks discrimination and divisiveness for no clear purpose

The immigration control exemption is completely separate to existing exemptions relating to crime, currently contained in Section 29 of the Data Protection Act 1998 and replicated in paragraphs 2 and 3 of Schedule 2 of this Bill. If the Home Office or other relevant data controllers believe that the fulfilment of their data protection obligations would prejudice the investigation of immigration crimes - such as those set out under Part III of the Immigration Act 1971, which include illegal entry and overstaying, or more recent offences created by the 2014 and 2016 Immigration Acts, such as illegal working or driving while unlawfully in the UK - they can already use the existing crime exemptions, which the Home Office readily does.

The Government has made no case for establishing a new exemption to data privacy rights for the maintenance of effective immigration control as an objective distinct from the investigation or prevention of immigration crime. Indeed, it has made no attempt to define this new objective at all. Nowhere in this Bill or its explanatory notes are the notions of effective immigration control, or the activities requiring its maintenance, defined. Lord Avebury mounted robust and ultimately successful opposition to clause 28 in 1983 on the basis that "'the control of immigration is a very wide concept indeed, greatly lacking in particularity."[22] His objections – and indeed those of several members of the House - have the same resonance now as they did at that time. Yet in this Bill, the Government has gone further still and included an exemption for controllers on a second but related ground: "the investigation or detection of activities that would interfere with effective immigration control."

It is virtually impossible to concoct an exhaustive list of all of the activities that might be included under this rubric, or of individuals who might be affected. The potential list of groups extends far beyond documented or undocumented migrants themselves. **For example, does running a night shelter or food bank that benefits undocumented**

[21] Lord Avebury, ibid.
[22] Lord Avebury, ibid.

migrants amount to an activity interfering with effective immigration control, to the extent that it frustrates the Home Office's stated strategy of incentivising voluntary returns through enforced destitution? Could the acquisition of a person's address from a trusted frontline service such as a school or hospital, without their knowledge, and before they have committed or been suspected of breaching immigration law, be facilitated under this exemption? And what would be the effect on migrants' willingness to engage with those trusted public services in the knowledge that this was possible, and that other personal data could be similarly acquired, even if they had no intention of committing breaching immigration law?

Moreover, this exemption could ostensibly be used be used to facilitate the sharing of personal data of any individual interacting with public services between those services, or intermediary Government departments, and the Home Office to check their entitlement to access those services in real time, **amounting in effect to a digital ID card**. This is precisely the state of affairs envisaged in a draft policy document, apparently emanating from the Home Office, leaked to *The Guardian* in September 2017. At paragraph 3.26, under the heading "an efficient digital process", the document states:

> "A key aim is to make the new immigration system as digital, flexible and frictionless for individuals and employers as possible. It will be supported by improved data sharing capabilities between government departments, notably between the Home Office, HM Revenue and Customs, and the Department for Work and Pensions, to link together tax, benefit and immigration records in a fully automated and digital way. A secure digital portal will enable employers and public service providers quickly to check the immigration status of an individual and take action if necessary."[23]

Making the new immigration system as "digital, flexible and frictionless" as possible is a laudable aim. However, given the breadth and depth of the intrusion into individuals' private lives that could be facilitated by this exemption, it is astonishing that apart from in this leaked document, no serious indication has been given as to the exemption's intended scope or purpose.

There is already evidence to suggest that existing data-sharing schemes administered by the Home Office involve a rate of error which, given the adversity of the consequences for affected individuals, who may well have leave to remain in the UK, should be considered significant. For example, the Immigration Act 2014 prohibits banks from opening current

[23] *The Guardian,* 'The draft Home Office post-Brexit immigration policy document in full', 5 September 2017 https://www.theguardian.com/uk-news/2017/sep/05/the-draft-home-office-post-brexit-immigration-policy-document-in-full

accounts for undocumented individuals, and requires them to use a third-party database to check individuals' eligibility. A 2016 investigation by the Chief Inspector of Borders and Immigration found that of a sample of 169 refusals to open bank accounts, 10% of refusals had been made in error.[24] One of those refusals involved a Jamaican national with leave to remain in the UK, who had been lawfully present in the country for over a decade. These errors are not confined to entitlement checks for current accounts. *The Guardian* recently reported[25] the case of Dr Mohsen Danaie, an Iranian-Canadian research scientist working for the UK's Diamond Light Source. He holds a valid work visa, due to run out in September 2019. In September this year, he received a letter from Home Office Immigration Enforcement telling him that he had "no lawful basis to be in the UK", that his driving licence would be revoked, and that he would be subject to forcible removal if he did not leave the UK voluntarily. The wrongful notification clearly was clearly the result of inaccurate records being held either by the Home Office or the DVLA, and shared between the two agencies without Dr Danaie's knowledge. As he reflects himself:

> "It [...] left me curious to know what exactly was the bureaucratic process behind the letter. How could they possibly get my name wrong, but my address right? Did someone just type that information off a physical dossier? How advanced is the infrastructure at the Home Office? Should we not fear for our safety?"

Poor data quality may lead to erroneous and distressing enforcement action being taken against individuals who have leave to remain in the UK. But crucially, the entrenchment and extension of the principle that individuals' personal data collected for one purpose can be used by Government for another without their informed consent sets a damaging precedent for the privacy rights of each and every one of us. To reuse data for a secondary, unconsented purpose that is incompatible with the original purpose would be a clear disregard of the very core of data protection in the UK. If paragraph 4 of Schedule 2 raises the spectre of the "fraud on the public" against which the Lindop Committee warned in 1983, the chilling fact is that that fraud is already a living, breathing and fundamental tenet of the Home Office's daily practice, and that of several other Government departments.

---

[24] Cifas is a third sector organisation that holds the UK's largest anti-fraud database. A data-sharing agreement between it and the Home Office is referenced at paragraph 6.29 in *Independent Chief Inspector of Borders and Immigration (ICIBI),* 'An inspection of the 'hostile environment' measures relating to driving licences and bank accounts' October 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567652/ICIBI-hostile-environment-driving-licences-and-bank-accounts-January-to-July-2016.pdf

[25] *The Guardian,* ''Leave UK immediately': scientist is latest victim of Home Office blunder', 26 September 2017 https://www.theguardian.com/uk-news/2017/sep/26/leave-uk-immediately-scientist-is-latest-victim-of-home-office-blunder

It is wholly unclear how it will be determined that the exercise of the rights listed at Schedule 2 paragraph 1 would genuinely prejudice immigration control or associated activities. In the absence of any feasible alternative, the data controller carrying out the immigration control or investigation activity would be the arbiter of whether fulfilment of an individual's rights under the Bill would undermine the objectives of the processing. And the individual whose data is being processed would have no opportunity to object to the application of the exemption to the processing of their data, because its very application precludes them exercising their right to know that their data is being processed in this way. In short, the Home Office and other agencies would have virtually untrammelled ability to acquire and process individuals' data from any other Government department, corporate or other entity without transparency or oversight even where there is no suspicion of criminality. The disquieting breadth of this exemption coupled with the Government's already problematic overreliance on existing law enforcement exemptions (discussed below) to acquire migrants' data poses too grave and discriminatory a risk to the privacy rights of millions to remain part of this Bill.

- The exemption removes any meaningful check on processing of data for immigration control purposes

The immigration control exemption removes any obligation under data protection law to inform an individual that their data has been transferred to the Home Office for immigration control purposes, or the investigation of activities that would undermine it. Individuals would therefore have no way of knowing that their data has been passed to the Home Office. They would consequently be unable to challenge any potential breach of law or ethics arising from the data transfer itself, in addition to being unable to exercise other rights, such as the right to know what information about them the Home Office has obtained, in what way it is being used for immigration control purposes, or to request that it be corrected if any part of it is inaccurate.

In making the case for clause 28 to be removed from the 1983 Bill, Lord Elwyn-Jones, arguing that it was "the most grave fault in the Bill", stated:

> "[I]t may well mean that highly confidential and sensitive information could be secretly disclosed to the police, the Inland Revenue, the Customs and Excise, and the immigration authorities, without any indication on the data protection register that anything of this kind was even possible. I must again remind the House of the

comment of the Lindop Committee which called it a fraud on the public – a grave allegation indeed."[26]

While clause 28 was ultimately dropped from the Bill, the hypothetical state that so alarmed Lord Elwyn-Jones, the Lindop Committee and many others has nevertheless come to pass. Current data-sharing arrangements for enforcement against immigration crime as concluded by the Home Office are typified by secrecy, total disregard for any of the fundamental principles currently governing data protection, and a wholesale failure to balance immigration enforcement objectives proportionately against competing public policy objectives or fundamental human rights. The operation of these schemes and their cumulative detrimental impact on individuals' lives, far from justifying any extension in the Home Office's ability to process personal data for immigration control as proposed by paragraph 4 of Schedule 2, points strongly towards the opposite: that the existing exemption on data protection obligations on law enforcement grounds should be narrowed to exclude low-level immigration crime.

Since 2012, the Home Office has operated with a public commitment to creating a "hostile environment"[27] for undocumented migrants. Its effects reverberate well beyond its stated target group to affect migrants with regular status, settled black and minority ethnic (BAME) communities, and indeed the very fabric of the society in which we live through the requirement it imposes on public servants and private citizens to check individuals' entitlements to goods and services, as well as the racially discriminatory impacts routinely felt by individuals who are subjected to the checks.

The widespread and routine sharing of personal data collected by frontline agencies with the Home Office forms the cornerstone of the hostile environment, and involves schools, NHS services, police, social services, banks, and the DVLA. Many of these data-sharing practices are codified by a series of MOUs concluded between various government departments and the Home Office, although some take place on an ad hoc basis. For the most part these agreements have been concluded in secret. Their existence has been brought to light primarily through Freedom of Information Act (FOIA) requests. Public awareness of them remains low, and parliamentary scrutiny of them has been negligible.

[26] Lord Elwyn-Jones, Data Protection Bill [H.L.] HL Deb 24 March 1983 vol 440 cc1236-86 http://hansard.millbanksystems.com/lords/1983/mar/24/data-protection-bill-hl#S5LV0440P0_19830324_HOL_186

[27] *The Telegraph*, 'Theresa May interview: 'We're going to give illegal migrants a really hostile reception', May 2012 http://www.telegraph.co.uk/news/uknews/immigration/9291483/Theresa-May-interview-Were-going-to-give-illegal-migrants-a-really-hostile-reception.html

Known bulk data-sharing schemes currently operate between the Home Office, the Department of Health (DoH) and NHS Digital;[28] the Home Office and the Department for Education (DfE);[29] the Home Office and Cifas;[30] the Home Office and the DVLA;[31] and the Home Office, the Department for Work and Pensions (DWP) and HMRC[32]. They have shared features to the extent that they operate to allow the Home Office to attempt to obtain from those agencies personal data, namely up-to-date contact details for individuals who are suspected of committing an immigration crime and with whom the Home Office has lost contact (NHS Digital/DoH, DfE, Cifas, DWP/HMRC), and/or they allow an agency to check an individual's immigration status with the Home Office when they attempt to access a good or a service, and provide up-to-date contact details to the Home Office when informed that a person is not entitled (Cifas, DVLA, DWP/HMRC). The Greater London Authority (GLA) also shares aggregated, sensitive personal data collected by homelessness outreach services with the Home Office to facilitate enforcement activity against non-UK rough sleepers, some of whom have committed no immigration crime, but under Home Office policy[33] are deemed to be misusing or abusing their EU treaty rights.[34] Ad hoc data-sharing practices by police on victims of crime have also been reported.[35] Across the board, individuals are not informed when they interact with frontline services that their data may be processed in this way, not least because many frontline workers are unaware of the existence of these data-sharing agreements.

[28] 'Memorandum of Understanding Between Health and Social Care Information Centre and the Home Office and the Department of Health' 27 September 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/585928/MOU_v3.pdf

[29] 'Memorandum of Understanding Between The Home Office And Department for Education In Respect of the Exchange Of Information Assets' 7 October 2016 http://defenddigitalme.com/wp-content/uploads/2016/12/20161016_DfE-HO-MoU-redacted-copy.pdf

[30] Cifas is a third sector organisation that holds the UK's largest anti-fraud database. A data-sharing agreement between it and the Home Office is referenced at paragraph 2.6 in *Independent Chief Inspector of Borders and Immigration (ICIBI),* 'An inspection of the 'hostile environment' measures relating to driving licences and bank accounts' October 2016 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567652/ICIBI-hostile-environment-driving-licences-and-bank-accounts-January-to-July-2016.pdf

[31] ICIBI, ibid.

[32] Agreements obtained by Liberty and journalists through FOI request, and referenced in *Vice Magazine*, 'Theresa May's 'Anti-Slavery' Agenda Is About Deporting Migrants' 21 September 2017 https://www.vice.com/en_uk/article/8x8qbv/theresa-mays-anti-slavery-agenda-is-about-deporting-migrants

[33] *Home Office policy guidance*, 'European Economic Area nationals: misuse of rights and verification of EEA rights of residence' 1 February 2017 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/588682/Misuse-of-rights-and-verification-of-EEA-rightsv2_0EXT.pdf

[34] Agreement obtained through FOIA by Liberty and reported on by *The Observer,* 'Home Office used charity data map to deport rough sleepers' 19 August 2017: https://www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-data-homeless-eu-nationals

[35] Politics.co.uk, *Met police hands victims of crime over to the Home Office for immigration enforcement,* 5 April 2017: http://www.politics.co.uk/news/2017/04/05/met-police-hands-victims-of-crime-over-to-the-home-office

The Government relies heavily on the crime exemption set out at Section 29 of the DPA 1998 to justify the operation of the majority of these schemes, as many aspects of the lives of undocumented people, such as working or driving, or simply being present in the UK without the requisite permission, are criminalised. However, it is far from clear that the agreements are lawful, and it is likely that some of the agreements, and especially those affecting essential public services such as schools, hospitals, GP's surgeries and social services, in whole or in part breach Articles 8 and 14 of the ECHR to the extent that they represent a disproportionate interference with individuals' right to privacy, and constitute a two-tier regime of confidentiality that is indirectly discriminatory on the basis of nationality. These agreements are also anathema to good government to the extent that they subordinate legitimate public policy aims such as the protection of public health, homelessness support, and child safeguarding, to immigration enforcement priorities.

As public awareness of existing data-sharing agreements grows, their effect can only be to force undocumented people to avoid sending their children to school, visiting the GP, presenting to homelessness services or seeking social support for fear that they risk detention and removal by doing so. The measures therefore have a damaging impact on children's right to education, individuals' right to health, and ultimately individuals' rights to life and to be free from inhuman and degrading treatment should medical conditions go untreated or child destitution fail to be remedied because people cannot present to the public services capable of supporting them.

To the extent that third sector agencies, private entities and public bodies are already obliged by other legislation to share data with the Home Office, or voluntarily enter into data-sharing agreements with it, this exemption represents a potentially huge expansion in the transfer of individuals' data for immigration control purposes. The exemption also opens the way to commercial datasets or even open data being acquired by the Home Office and processed for immigration control purposes without any affected individual's knowledge, consent, or opportunity to ensure that the data acquired is accurate. Yet the Government has not provided any explanation as to why such processing must take place without individuals being able to access their basic rights as data subjects, including the rights to know about and consent to such processing.

- The exemption's effect on individual's ability to access their own data

The immigration control exemption also means data controllers, including the Home Office, would not be obliged to respond to subject access requests (SARs) from people wishing to know what data about them is retained, if the Home Office determines that responding would engage the exemption. SARs are used by legal practitioners to acquire information necessary to advise individuals, and particularly undocumented individuals, as to their current immigration status and to give further legal advice to an individual on that basis, especially in circumstances where people no longer have their own record of previous representations. The effects of the loss of this right will be devastating.

Existing Home Office practice in failing to fulfil SARs fully and in a timely way already produces significantly deleterious effects for lawyers and their clients. The Joint Council for the Welfare of Immigrants (JCWI) conducted a survey to assess to what extent this was evidence of a systemic issue. In May 2017 it wrote[36] to the Information Commissioner's Office (ICO) requesting an urgent review of Home Office practice in fulfilling its Data Protection Act obligations on the basis of its findings. As JCWI states in its letter to the ICO:

> "All 42 respondents had experienced issues with Home Office staff failing to provide full or adequate disclosure to SARs[…]. Crucially, 26 of the 42 respondents stated that this happened every single time they made a SAR. A further 5 indicated that this happened almost every time, or the majority of the time. Of the 9 remaining respondents most indicated that this was something that occurred on a regular basis."[37]

JCWI further sets out the human and procedural cost of these failures, stating that

> "Combined with breaches of the 40-day time limit [these failures mean that] immigration cases often cannot progress expeditiously. The information needed for a client's case is often only available on the Home Office file, and the Home Office failure to disclose that information makes it impossible for the case to progress.
>
> Our respondents reported the following impacts of this practice:

- It prolongs periods of destitution for vulnerable migrants such as asylum seekers. This results in immense hardship to vulnerable people, including causing street homelessness;

[36] *Joint Council for the Welfare of Immigrants,* 'Letter to the Information Commissioner's Office', 5May 2017 [unpublished, seen by Liberty].
[37] JCWI, ibid.

- Without the file the client's immigration history is unclear, so they cannot be advised to their status, and remain vulnerable;
- Clients in immigration detention are particularly impacted by this inability to advise, as the uncertainty is even more damaging when their liberty hangs in the balance."[38]

The proposed immigration control exemption will likely multiply these effects on an exponential scale. It will prevent those with unclear or precarious status from regularising their status, which is surely an activity that the Home Office wishes to encourage in its work to maintain effective immigration control. In this regard, the exemption is not only deeply damaging to the individuals affected, it is also self-defeating.

Adequacy in jeopardy? Compliance of Schedule 2 paragraph 4 with the GDPR

The Government's future partnership paper on the exchange and protection of personal data[39] outlines its desire to ensure that the UK's data protection framework is adequate for the free flow of data between the UK and the European Union (EU) to continue after the UK leaves the EU in March 2019. But the inclusion of an immigration control exemption in the Bill jeopardises that entire endeavour. The Government seeks to rely on Articles 23(1) of the GDPR in creating the exemption. Article 23(1) reads (emphasis added):

> "Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, **when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society** to safeguard:
>
> (a) national security;
>
> (b) defence;
>
> (c) public security;

[38] JCWI, ibid.
[39] *HM Government*, 'The exchange and protection of personal data: a future partnership paper' 24 August 2017: https://www.gov.uk/government/publications/the-exchange-and-protection-of-personal-data-a-future-partnership-paper

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims."

Moreover, where such exemptions are created, Article 23(2) of the GDPR stipulates that:

"2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction."

As emphasised above, the GDPR only permits such exemptions when they respect the essence of the fundamental rights and freedoms, and to the extent that they represent a necessary and proportionate measure in a democratic society to protect one of the legitimate aims listed at Article 23(1)(a-i). Immigration control is not listed as a legitimate aim in its own right, and as set out above the Government has not established what immigration control actually consists in, distinct from the prevention or investigation of immigration crime. Even if immigration control can be established as a legitimate aim subsidiary to one of the aims set out at 23(1)(a-i), to the extent that as argued above, the exemption establishes an inferior data protection regime that is indirectly discriminatory on the grounds of nationality, it is plainly an affront to the essence of the fundamental rights to privacy and to freedom from discrimination, as well as being wholly disproportionate in light of the intrusive monitoring of migrants' lives and unfettered data-sharing between agencies that it enables. And last, even if the exemption did not fly in the face of individuals' fundamental human rights, the Government has failed to fulfil the majority of the procedural requirements governing exemptions under Article 23(1) as required by Article 23(2), and especially at (b)-(h). Thus the pursuit of adequacy in data protection arrangements, like so many other important public policy objectives, is defeated by the Government's attempt to bring border controls into every aspect of our lives no matter the cost.

Powers delegated to the Secretary of State

Amendments

Delegated powers to amend safeguards for processing of sensitive personal data

Clause 9, page 5, line 42, leave out sub-sections (6) and (7).

Delegated powers to make further exemptions from data rights

Clause 15, page 8, line 35, leave out Clause 15.

Delegated powers to amend safeguards for processing of sensitive personal data for law enforcement

Clause 33, page 20, line 14, leave out sub-section (6).

Delegated powers to amend safeguards for processing of sensitive personal data by intelligence services

Clause 84, page 49, line 17, leave out sub-section (3)

Delegated powers to make further exemptions from data rights regarding intelligence services processing

Clause 111, page 61, line 13, leave out Clause 111.

Effect

These amendments would remove from the Bill excessively broad delegations of law-making power to the Secretary of State. Removing Clauses 15 and 111 would prevent the Secretary of State subverting Parliament's judgment and circumventing robust Parliamentary review of the scope of proper derogations from data privacy rights. Removing Clauses 9(6)-(7), 33(6) and 84(3) would keep with Parliament any power to alter the legislative determination of the proper balancing of individual privacy and public and social interests in the processing of sensitive personal data set forth in Clause 9 and Schedules 1, 8 and 10.

Briefing

In its current form, the Data Protection Bill grants unacceptable power to Ministers to introduce secondary (subordinate) legislation that bypasses parliamentary control over decisions to derogate from data privacy rights and undermines the Bill's comprehensive legislative scheme for determining the balance between data privacy and other important rights and social purposes.

Clauses 15 and 111: Loopholes Calling the Entire Bill Into Question

One of the key purposes of this Bill is to strike a balance between individuals' rights to data privacy and the proper use of use data by defining and delimiting the legitimate reasons that people's data may be collected and processed, and setting important procedural safeguards on that collection and processing.

To that end, Schedules 2, 3, 4, and 11 of the Bill set forth several categorical exemptions to the individual data privacy rights granted under GDPR. In this briefing, Liberty has taken issue with a number of these exemptions, illustrating—at a minimum—their significance and the importance of debate in Parliament on defining their scope.

But Clauses 15 and 111 of the Bill would grant to the Secretary of State power to redefine the scope of the Bill's exemptions—and even to create entirely new exemptions—for a broad range of reasons. Among these reasons is an open-ended mandate to formulate "new legal bases for the performance of tasks in the public interest or in the exercise of official authority." This Clause gives the Executive power to rewrite or even delete any part of Clause 14 or Schedule 2, 3, 4 and 11 of the Bill – arguably the heart of the Bill—as well as to add any new national security-based exemption to Part 4 of the Bill as the Secretary of State desires.

With clauses like this, why legislate at all?

Notably, a similarly broad delegation of authority was soundly defeated in the Labour Government's Coroners and Justice Bill 2009. Clause 152 of that Bill would have permitted ministerial "information-sharing orders" to share information among ministries in circumstances similar to those in which this Bill permits new derogations from privacy rules.[40] Dominic Grieve MP, then Shadow Secretary of State for Justice, denounced the clause as a "seismic change in the relationship between the State and the citizen" with potential to enable an "oppressive state."[41]

It is true that the delegated powers in this Bill are limited to grounds for exemptions acknowledged in certain provisions of the GDPR. But those GDPR provisions are meant to create space for democracies to resolve important conflicts among rights, interests and

[40] O. Butler, The Data Protection Bill and Public Authority Powers to Process Personal Data: Resurrecting Clause 152 of the Coroners and Justice Bill 2009?, U.K. Const. L. Blog (28th Sept. 2017) (available at https://ukconstitutionallaw.org/2017/09/28/oliver-butler-the-data-protection-bill-and-public-authority-powers-to-process-personal-data-resurrecting-clause-152-of-the-coroners-and-justice-bill-2009/)
[41] https://publications.parliament.uk/pa/cm200809/cmhansrd/cm090126/debtext/90126-0007.htm

duties in the manner than best fits their national culture and legal framework. The resolution of such important conflicts should be the domain of Parliament, through robust democratic process. Parliament should not abdicate this responsibility to the Secretary of State by granting the Executive this broad power.

Clauses 9(6), 33(6) and 84(3): Undermining a Comprehensive Legislative Scheme for Processing Sensitive Personal Data

The provisions of the Bill governing the processing of sensitive personal data replicate the problem described above in a more specific context.

Clause 9 and Schedule 1 of the Bill create a comprehensive legislative scheme governing the processing of particularly sensitive categories of personal data. Those categories of data include:

- Data revealing racial or ethnic origin
- Data revealing political opinions, religious or philosophical beliefs, or trade union membership
- Genetic data, or biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerns criminal convictions and offences or related security measures
- Data concerning a person's sex life or sexual orientation.

Consistent with the GDPR, Clause 9 and Schedules 1 of the Bill together allow processing of this data for restricted, defined purposes. Those purposes include:

- When necessary to obligations or rights under employment, social security or social protection laws (Clause 9(2); Schedule 1, Part 1(1));
- When necessary for health or social care purposes – specifically, preventative or occupational medicine, assessments of working capacity, medical diagnosis, provision of health care or treatment, provision of social care, or the management of health or social care systems or services (Clause 9(2); Schedule 1, Part 1(2));

- When necessary for public health and carried out by a health professional or another person who owes a duty of confidentiality to the subject (Clause 9(2); Schedule 1, Part 1(3));

- When necessary for archiving, research or statistical purposes that are in the public interest (Clause 9(2); Schedule 1, Part 1(4));

- When necessary to a substantial public interest – specifically, parliamentary, statutory or government purposes; equality of opportunity or treatment; preventing or detecting unlawful acts; protecting the public against dishonesty; journalism in connection with unlawful acts or dishonesty; preventing fraud; suspicion of terrorist financing or money laundering; counselling; insurances; third party data processing for insurance purposes; occupational pensions; political parties; various functions relating to elected representatives; and anti-doping in sport. (Clause 9(3); Schedule 1, Part 2);

- When processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is acting in its judicial capacity (Schedule 1, Part 3)

- To facilitate a subject's membership in a political, philosophical, religious or trade union organisation (Schedule 1, Part 3);

- Where the subject has given consent, or is not capable of giving consent but processing is in the subject's vital interests (Schedule 1, Part 3); and

- Where the information is already in the public domain (Schedule 1, Part 3).

Schedule 1 of the Bill also places procedural protections on permissible processing of sensitive personal data for these enumerated purposes. For example, in some instances it requires the controller to document how the processing will be tailored narrowly to its specific purpose; how it will be processed lawfully, accurately, transparently and fairly; how long the data will be retained; and how it will be kept secure. (Schedule 1, Part 4 (incorporating GDPR Article 5 and 6)).

In the case of the public interest purpose – the broadest of the permissible purposes for processing sensitive personal data under Clause 9 – Schedule 1 places nine pages of additional limiting criteria and procedural requirements on such processing for each of the defined sub-categories of "public interest." (Schedule 1, Part 2, pages 113-121).

But Clause 9(6) gives the Secretary of State power to upend this legislative scheme. That clause permits the Secretary of State to use subordinate legislation to unilaterally amend,

vary or eliminate virtually all of the limitations, conditions and criteria governing the processing of sensitive personal data for these specified purposes. It further allows the Secretary of State to make any amendments deemed "consequential" to Clause 9. Any regulations made using this power would be subject to only minimal Parliamentary scrutiny through the affirmative procedure.

The Government justifies this power by pointing to the fact that it used a similar power five times to add processing conditions for sensitive data to the Data Protection Act 1998.[42] But, the use of an amending power five times over nearly a decade hardly suggests the need for delegated power in lieu of normal Parliamentary consideration. All of those changes are now incorporated into this Bill, which reflects not only a decades' of UK experience implementing data privacy regulations, but also the insights of the entire European Union reflected in the GDPR.

Beyond this justification, the Government points vaguely to the need to "update" the rules to respond to "changing circumstances."[43] But the Government neither suggests what circumstances might change nor explains why it should be up to the Secretary of State rather than Parliament to respond. It is for Parliament to decide, in this Bill, how to strike the balance between individual privacy and the valid reasons for processing sensitive personal data. Parliament should not abdicate that responsibility and empower the Executive to fundamentally recalibrate the approach.

This delegation over authority is even more unprecedented when considered in the context of the pending EU (Withdrawal) Bill, which, in combination with this Bill, would undermine the GDPR as a check on the misuse of ministerial authority to undermine data privacy rights. The EU (Withdrawal) Bill gives ministers power to use any power to make subordinate legislation to amend any "retained EU law" – which would include the GDPR itself.[44] That Bill also would eliminate important data privacy rights contained in the Charter on Fundamental Rights, Article 8.[45] Through both these Bills, the Executive would arrogate to itself the power to eliminate rights-based barriers to the exercise of governmental power to process sensitive, private, individual data. Parliament should not cede such unprecedented power.

---

[42] Delegated Powers and Regulatory Reform Committee, Data Protection Bill: Memorandum by the Department for Digital, Culture, Media and Sport and the Home Office (14 Sept 2017) at p. 5-6, paragraphs 23-24 (available at https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066-DPM.pdf)

[43] *Id.* at p. 6, paragraph 25.

[44] European Union (Withdrawal) Bill, Schedule 8, paragraph (3), page 50, line 2.

[45] European Union (Withdrawal) Bill, Clause 5(4), page 3, line 20. As the court noted in *Davis v. Secretary of State for the Home Department* [2015] EWHC 2092, the Charter "clearly goes further, is more specific, and has no counterpart" in other privacy laws.

For these reasons, Liberty recommends deleting Clause 9(6). For the same reasons, Liberty recommends deleting Clauses 33(6) and 84(3), which mirror Clause 9(6) in granting the Secretary of State power to amend Schedule 8 and Schedule 10, the counterparts to Schedule 1 for rules governing processing of sensitive personal data by law enforcement and intelligence agencies.

Gracie Bradley

Silkie Carlo

Corey Stoughton