



Joint Committee on Human Rights

Committee Office · House of Commons · London · SW1A 0AA

Tel 020 7219 2797 Email JCHR@parliament.uk Website www.parliament.uk



From Rt Hon Harriet Harman MP, Chair

Rt Hon Matt Hancock MP
Secretary of State for Health and Social Care
39 Victoria Street
London
SW1H 0EU

29 May 2020

Dear Matt

Re: Digital contact tracing protections

Thank you for your reply on 21 May in which you reiterate your view that new legislation to protect data gathered under the Test Trace Isolate programme is not necessary and in which you declined to adopt our Bill.

We remain concerned that the assurances that you gave to us about data protection are not met in the current legal framework and to assist you we have undertaken a comparison between the protections currently in place and those afforded by our Bill.

It is not possible to maintain the case that the current patchwork of protections is adequate to protect privacy under this necessary but unprecedented data gathering exercise. These new powers require new protections and I'd be grateful if you would consider this analysis and in light of it reconsider your decision to reject the Bill.

It is important as a matter of principle for the government to do all it can to protect the privacy of its citizens. It is important, too, that the battle against the pandemic is not undermined by a collapse in confidence caused by a data breach. The Bill we have presented to you enables you to fulfil your responsibilities on both counts.

Yours sincerely

Rt Hon Harriet Harman QC MP
Chair of the Joint Committee on Human Rights

DIGITAL CONTACT TRACING PROTECTIONS: A COMPARISON BETWEEN PROTECTIONS UNDER THE DIGITAL CONTACT TRACING (DATA PROTECTION) BILL AND THE EXISTING SITUATION UNDR THE DATA PROTECTION ACT

	ISSUE	Digital Contact Tracing (Data Protection) Billⁱ	Data Protection Act and (UK) General Data Protection Regulation
1	PURPOSE OF DATA COLLECTION & USE	Data may <u>only</u> be collected and used for the purpose of preventing or controlling the spread of Coronavirus. To do otherwise is a criminal offence.	Provided an individual gives consent to the sharing of their data, there are few restrictions on data collection and use beyond basic data principles, which require data is only processed for the specified purpose (the principle of purpose limitation). The key difference is that the DPA does not require any particular purpose. The Government could decide to use a wide or vague purpose when gaining consent for the app and even change that purpose for future users of the app.
2	WHO HAS ACCESS TO DATA	Data may only be accessed by persons specifically authorised to do so for the purpose of preventing or controlling the spread of Coronavirus. To do otherwise is a criminal offence. The specific persons will be listed in an annex to the Act which any member of the public can access.	There are no specific restrictions on data access beyond basic data principles. This could allow personal data to be shared with anyone as long as it is necessary for the stated purposes and not contrary to the consent given by individuals.
3	TIME LIMITS FOR RETAINING DATA,	Data may only be retained in line with published arrangements made in consultation with the Digital Contact Tracing Human Rights Commissioner.	Data retention is not subject to any specific or clear time limits beyond basic data principles which require data is kept no longer than is necessary to the purposes it is processed (principle of storage limitation). If the stated purpose is wide (for example for the prevention of future virus outbreaks) then some data could be retained for years or even indefinitely.
4	ANONYMISATION AND DELETION OF DATA	Data may only be retained centrally for as long as needed and must be deleted upon request. Data held must be anonymised in a way that prevents re-identification	There is no explicit requirement to delete data upon request. From evidence given to the JCHR, there is ambiguity as to whether data will be used for reidentification (data reconstruction). There is no

DIGITAL CONTACT TRACING PROTECTIONS: A COMPARISON BETWEEN PROTECTIONS UNDER THE DIGITAL CONTACT TRACING (DATA PROTECTION) BILL AND THE EXISTING SITUATION UNDR THE DATA PROTECTION ACT

		when combined with other data.	specific undertaking to ensure that data is not capable of data reconstruction.
5	ACCOUNTABILITY TO PARLIAMENT	Government is required to undertake regular reviews (every 21 days) on the efficacy, privacy, discrimination, human rights, complaints and security aspects of digital contact tracing and to report to Parliament on those reviews.	No requirement for reviews, information about the app or reporting to Parliament.
6	SECURITY	National Cyber Security Centre must regularly (at least monthly) review and certify the security of data held.	There is no explicit requirement on data security beyond basic data principles (principle of integrity and confidentiality) which require that the Government ensures appropriate security.
7	TRANSPARENCY	There are specific requirements for the Government to publish information relating to the design, security, ethics and data protection impact assessments relating to digital contact tracing.	There are no explicit or detailed transparency obligations beyond the basic data principles (principle of lawfulness, fairness and transparency), which require that data is processed in a “transparent manner”.
8	OVERSIGHT & MONITORING	Establishes a Digital Contact Tracing Human Rights Commissioner to oversee and monitor privacy, human rights and discrimination issues related to digital contact tracing	The Information Commissioner has existing powers relating to privacy. However, these rely on the more flexible controls in the Data Protection Act / General Data Protection Regulation.
9	LEGAL CERTAINTY AND CLARITY	Sets out clearly in law what data will be gathered, for what purpose, who can access, when it will be deleted and what reporting and oversight mechanisms are in place.	There is less certainty as reliance is placed on changing Government policies about what data they are gathering, who can access it, when/whether it will be deleted and has less reporting and oversight

DIGITAL CONTACT TRACING PROTECTIONS: A COMPARISON BETWEEN PROTECTIONS UNDER THE DIGITAL CONTACT TRACING (DATA PROTECTION) BILL AND THE EXISTING SITUATION UNDR THE DATA PROTECTION ACT

10	STOPPING DIGITAL CONTACT TRACING WHEN NO LONGER REQUIRED	There is an obligation to stop digital contact tracing when it becomes no longer necessary or proportionate for the purposes of preventing or controlling Coronavirus and to delete all data collected.	It is unclear when or how digital contact tracing, and the use of the data collected from it, will end. There is a suggestion from evidence given to the JCHR that some data could be retained indefinitely.
----	---	---	--

ⁱ NB All protection in the Digital Contact Tracing (Data Protection) Bill would apply on top of (i.e. in addition to) the protections in the Data Protection Act 2018 and the General Data Protection Regulation.