Sneaking in unnecessary and unaccountable 'national security' powers for police and the Home Secretary

Rights & Security International's briefing on the Data Protection and Digital Information (No. 2) Bill

The government is marketing the Data Protection and Digital Information (No. 2) Bill ('the Bill') as business-friendly, allowing businesses to use personal data in a more convenient way than under the Data Protection Act 2018 (DPA).

But this is not the full story.

The Bill is also a power grab: it would give the government and police significant, new and unaccountable powers to invade the personal lives of people in the UK, potentially on a massive scale.

Giving broad, unnecessary and unaccountable powers to police and the Home Secretary

Clauses 24-26 of the Bill would give the Home Secretary great and unaccountable powers to authorise the police to violate our privacy rights. The Bill would do this through two means: a shift in what the Home Secretary can do by using 'national security certificates', and a new regime of 'designation notices'.

Under clause 24(7), the Home Secretary would be able to issue a 'national security certificate' to tell the police they do not need to comply with many important data protection laws and rules that they would otherwise have to obey. For instance, a 'national security certificate' would give the police immunity when they commit crimes by using personal data illegally – and they will no longer need to respond to requests under the Freedom of Information Act.

The government has not tried to explain why it thinks police should be allowed to break the law and operate in darkness.

The Bill would also expand what counts as an 'intelligence service' for the purposes of data protection law, again at the Home Secretary's wish. Clause 25 would allows the Home Secretary to issue a 'designation notice' allowing law enforcement bodies to take advantage of the more relaxed rules in the DPA otherwise designed for the intelligence agencies, whenever they are collaborating with the security services. The government argues that this would create a 'simplified' legal framework, without acknowledging that it could hand massive amounts of people's personal information to police. This could include the private communications of people in the UK as well as information about their health histories, political beliefs, religious beliefs and sex lives, for example.

Stopping the courts, Parliament and individuals from challenging illegal uses of personal data

Both the amended approach to 'national security certificates' and the new 'designation notice' regime would be unaccountable: the courts would not be able to review what the government is doing, and therefore Parliament might never find out.

National security certificates are unchallengeable before the courts, meaning that the police and the Home Secretary would be unaccountable if they abused these powers. If the Home Secretary says that the police need to use these increased – and unnecessary – powers 'in relation to' national security, then her word will be final. This includes the power to commit crimes.

Designation notices are also a power grab. The Home Secretary is responsible for approving and reviewing their use. Only a person who is 'directly affected' by a designation notice will be able to challenge it – yet the Home Secretary would have the power to keep the notice secret. In which case, how could anybody know that the police have been snooping on their lives under this law?

Violating the right to privacy under human rights laws – and setting up court fights

Clauses 24-26 could violate UK's obligations under the Human Rights Act and the European Convention on Human Rights (ECHR), including because they remove the courts' role in reviewing how the government uses its surveillance powers. This would set the government up for legal battles in the UK and at the European Court of Human Rights about its data protection and surveillance regimes. It could also harm important relationships the UK has with the EU around data.

Under the ECHR, the UK government must ensure that everything it does, including in the name of national security, complies with human rights laws. This means it must make sure that anytime it interferes with the privacy of people in the UK, it obeys the law, has a legitimate goal and only does what is truly necessary to achieving that goal. The government has not shown why limiting our rights would be necessary and the least intrusive option. Instead, it has talked about convenience – but it is not allowed to cut out the courts and Parliament, and let police commit crimes, simply because it thinks this is convenient.

Clauses 24-26 would grant the government and police broad and unaccountable powers with virtually no possible restraint from the courts. We urge the government to withdraw them from the Bill.

About Rights & Security International

Rights & Security International is a London-based charity working to eliminate human rights abuses committed in the name of national security. We challenge religious, racial and gender bias in national security policies, and advocate for justice and transparency for victims of human rights abuses.