The UK government's lesson from years of police snooping? Give them more powers

Rights and Security International's opposition to clauses 87-89 of the Data (Use and Access) Bill

Police in the UK have a long history of misusing our personal data: for example, the ongoing Undercover Policing Inquiry is investigating allegations of misconduct by undercover police units, and another investigation found seven Metropolitan Police officers guilty of gross misconduct for accessing the personal data of the murdered Sarah Everard.

The government's lesson learned from years of abusive police snooping? Apparently, to give the police more powers, and ensure that they cannot be held accountable for breaking the law.

The prior government had tried to do the same thing, but MPs, peers and civil society groups (including RSI) pushed back on the proposal for increased surveillance powers for police. However, instead of listening to these concerns, this government has simply reintroduced the same provisions that Parliament refused to pass when they were in the Data Protection and Digital Information (No. 2) Bill (DPDIB) – the piece of legislation that the prior government tried to pass in 2023-2024. Neither government has ever shown that these powers are necessary – and if so, for what.

Especially without a showing of necessity, these powers would violate the Human Rights Act and be ripe for a legal challenge.

Clauses 87-89 of the Data (Use and Access) Bill are unnecessary, violate our rights, and create a risk of abuse. MPs should call on the government to scrap clauses 87-89 of the Bill.

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

Clauses 87-89 of the Bill would give the Home Secretary broad and unaccountable powers to authorise the police to violate our 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 87, the Home Secretary would be able to issue a 'national security certificate' to tell the police that they do not need to comply with 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 police would no longer need to respond to subject access requests under the Freedom of Information Act.

The Bill would also expand what counts as an 'intelligence service' for the purposes of data protection law, at the Home Secretary's discretion. Clause 88 would allow the Home Secretary to issue a 'designation notice' that allows police to take advantage of the more relaxed rules in the Data Protection Act otherwise designed for the intelligence agencies, whenever police say they are collaborating with the security services. This step could hand massive amounts of personal information about people in the UK to the police, such as private communications as well as information about people's health histories, political and religious beliefs and sex lives.

Police are human, and handing them sensitive data creates real risks of abuse and exploitation – including of women and minorities – no matter what amount of training they undergo.

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 would never find out.

National security certificates are unchallengeable before the courts. If the Home Secretary says that the police need to use these increased powers 'when required' for national security reasons, then their word will be final.

Designation notices are also a power grab. Only a person who is 'directly affected' by a designation notice will be able to challenge it, yet the Home Secretary – who is responsible for approving and reviewing their use – 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?

Violating the right to privacy under human rights law

Clauses 87-89 would violate UK's obligations under the Human Rights Act and the European Convention on Human Rights (ECHR). This is because there is no demonstrated necessity for them; they could also violate these obligations on the grounds that they hand unfettered discretion to the Home Secretary, and remove the courts' role in reviewing how the government and police use their surveillance powers. These problems 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 at a systemic level.

The Bill states that the police can interfere with our rights 'when required' for national security purposes, and the government has stated that these changes will 'simplify data protection considerations' for law enforcement and address the 'challenges to operational working' that are presented by separate data protection regimes. First, making data protection violations legal and providing immunity for what would otherwise be crimes is not 'simplifying': it amounts to throwing away important protections that exist for a reason. Second, vague statements about what is 'required' are not enough to make a measure 'necessary' for purposes of the ECHR; nor is it enough to say that a measure will make data processing more efficient. This is an issue Lord Anderson of Ipswich raised during debates about the DPDIB, asking:

'Does "required" mean the same as "necessary" or something different? Do the restrictions not need to be proportionate anymore? If so, why?'[1]

The government cannot allow the police to grab and use sensitive information about people without accountability just because it might make their jobs easier. Such a practice would make abuses easier as well.

The dangers of unaccountable surveillance powers

There is a long history of UK police interfering unlawfully with our right to privacy, which can have real consequences for the lives of victims.[2] An officer with access to personal information could easily stalk or blackmail that person, or use it as the basis for degrading conduct such as the misogynistic or homophobic sharing of photos or messages.[3]

For example, a recent internal investigation by the Metropolitan Police found that four serving and three former officers had accessed and shared murder victim Sarah Everard's personal data 'without proper reason' – in possible breach of data protection law – and that they had done so merely 'out of curiosity'.[4] Similarly, a 2022 investigation found that a Lincolnshire Police officer had repeatedly accessed policing records 'without a policing purpose' and merely to satisfy their 'curiosity', and had shared these records with their partner and, in one incident, with a suspect.[5] These scandals illustrate the obvious: sensitive data represents a large temptation, and some officers will use that data illegally if given the opportunity. There is no reason to grant immunity for such misconduct.

[1] Hansard, Data Protection and Digital Information Bill, Monday 15 April 2024, Col 287

[2] Shanti Das (2023) 'Revealed: Metropolitan police shared sensitive data about crime victims with Facebook' *The Guardian* 15 July 2023; Jon Ungoed-Thomas (2024) 'Police unlawfully storing images of innocent people for facial recognition' *The Guardian* 8 December 2024

[3] *The Guardian* 23 December 2023; Margaret Davis (2022) 'Racist, sexist and homophobic messages exchanged by Met Police officers exposed' *The Independent* 1 February 2022

[4] Tom Ambrose (2024) 'Police viewed sensitive files on Sarah Everard out of 'curiosity', panel hears' *The Guardian* 28 October 2024

[5] Paul Whitelam (2022) 'Former Lincolnshire Police officer shared personal data with partner and suspect' *Lincolnshire Live* 21 February 2022

Under the Bill, the Home Secretary could grant the police the power to violate our privacy rights, in secret and without oversight by Parliament, the courts, or affected individuals. The Undercover Policing Inquiry (responding to the 'spy cops' allegations) has evidenced the kinds of harmful surveillance powers that have previously allowed police to violate our privacy rights, with no accountability until many decades later. The spy cops scandal highlights the harms of giving the Home Secretary unaccountable and secretive powers to allow the police to commit crimes; meaning that we cannot challenge the misuse of our data until the damage is already done – if we are made aware of it at all.

Clauses 87-89 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.