Open Rights Group briefing on the National Fraud Initiative data matching powers consultation proposals

The UK Government has published proposals to extend the National Fraud Initiative (NFI) data matching powers - Consultation on the expansion of the National Fraud Initiative Data Matching Powers and new Code of Data Matching Practice[1] - which sets out a range of proposals that would dramatically expand data sharing powers in the public sector.

Of particular concern is the extension of data matching powers to allow police to use the service for the detection and prevention of any crime, without any restraints on what information they can request to ensure this is necessary and proportionate such as independent authorisation.

This briefing identifies the issue, provides context and summarises Open Rights Group's (ORG) main concerns about the proposals.

ORG has written to the Head of the NFI and the Minister for the Cabinet Office expressing concerns about how the proposals are likely to impact migrants specifically:

- The lack of sufficient safeguards
- The volume of data being shared about migrants that could lead to abusive behaviour from authorities
- The extension of the powers for crime and offenders, expanding the capacity of police to collate information from public and private bodies

Introduction

The Cabinet Office's National Fraud Initiative (NFI) has published deeply worrying proposals to expand data matching which are likely to disproportionately intrude on fundamental rights. Last month, Open Rights Group (ORG) along with other privacy advocates and migrants' rights groups wrote to the NFI to express our concerns about the proposals.[2] We expressed concerns regarding the measures proposed and also the length of time given for different stakeholders to respond to the consultation. We felt it was insufficient given the expanded scope of these powers. We believe that the proposals as they currently stand are likely to impact the data protection rights of vulnerable and marginalised groups specifically migrants negatively and disproportionately, but also should concern anyone worried about due process and potentially excessive police powers.

What is the NFI?

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972419/2021-01-28-FINAL-NFI-New-Purposes-Consultation-document-v1.2-Version-control-added.pdf

[2] https://www.openrightsgroup.org/publications/joint-letter-to-national-fraud-initiative-re-consultation-extension/

The NFI is 'an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud'.[3] It is managed by the Cabinet Office.

Issue

At present, the National Fraud Initiative (NFI) collects more than 20 data types, over 8000 datasets, which is over 300 million data records from 1300 participant organisations.[4] Examples of datasets collected include: public sector payroll, housing benefit, social housing waiting lists, parking permits, council tax, local authority pension payments, electoral register, right to buy, public sector housing.[5] This massive data exercise at present is limited to combatting fraud. The proposals will change this in some really concerning ways.

Migration groups should be very concerned because the existing data sharing already involves checks on migration status and sharing of data with the Home Office. Hundreds of Tier 1 migrants have been denied indefinite leave to remain (ILR) after being accused of deceptive behaviour due to minor tax discrepancies and clerical errors,[6] under paragraph 322(5) of the immigration rules.[7] According to immigration specialist lawyers, these cases are "are amongst the most challenging to win".[8] Expanding this regime to all the other purposes will mean a lot more data being shared about migrants and new opportunities for abusive behaviour from authorities.

People concerned about the administration of justice should be concerned that such a wide power is to be granted to the police. The potential for inappropriate usage, targeting of individuals or groups, is vastly expanded.

This is exacerbated by the lack of external oversight for requests. Police are granted, in effect, a blanket power to gain any information currently collected for fraud investigations, without needing to gain permission. For phone data, for instance, the police must seek an external permission from the Office of Communications Data Authorisations.

The proposals are part of the Government's 'Consultation on the expansion of the National Fraud Initiative Data Matching Powers and new Code of Data Matching Practice.' The powers would be introduced by ministers through secondary legislation in an affirmative statutory instrument (SI) and both House of Parliament have to approve them. It's important to note that similar initiatives in the past have been soundly rejected by both Parliament and public opinion. The Government is consulting on its proposals, so you can have your say on whether the NFI should widen the data matching powers to assist with the:

- prevention and detection of crime (other than fraud);
- apprehension and prosecution of offenders;
- prevention and detection of errors and inaccuracies; and
- recovery of debt owing to public bodies

In addition, responses are also being sought to the following questions:

- Do you want to raise any particular equality related issues in relation to this proposal?
- Do you have any views on the updates to the Code of Data Matching Practice?

---

[3] https://www.gov.uk/government/collections/national-fraud-initiative

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972419/2021-01-28-FINAL-NFI-New-Purposes-Consultation-document-v1.2-Version-control-added.pdf

[5] Ibid

[6] http://righttoremain.org.uk/refusals-of-ilr-due-to-tax-discrepancies/

[7] http://www.gov.uk/guidance/immigration-rules

[8] http://ayjsolicitors.com/uk-personal-immigration-services/deception-cases-ilr-tax-issues-uk

- Do you have any views on the proposals to extend the data matching purposes with respect to data protection?

Background

The Government claims that the proposals will increase efficiency and improve the use of data in the process of government. It is difficult not to consider the proposals in the wider context of the Government's stated desire to increase the collection and sharing personal data and what this means for privacy, civil rights and civil liberties. We've already seen the Government pursue data-sharing practices for immigration enforcement.

According to the Royal Society:

'Since 1999, the topic of Government data sharing alone has, wholly or partly, been the subject of: three Government reports, an independent review, an 'open policymaking' process and a public consultation, two white papers, three acts, two codes of practice, and has provoked, in part at least, the creation of the Government Digital Service.'[9]

This has intensified during the pandemic and the UK government has been described as wanting 'pandemic levels of data sharing to be the new normal.'[10] Nowhere was the desire for increased data sharing more evident than in the National Data Strategy launched last year. The Government has been extremely keen to explain what benefits will be reaped by businesses, government and organisations by accelerating data sharing. However, it has been less keen to address the risks that this poses and detail what safeguards it would put in place to mitigate against these.

Main concerns

These are some of the issues raised by these new powers:

Unchecked increase in police powers

The most problematic issue in the proposals is the extension of the powers for crime and offenders, expanding the capacity of police to collate information from public and private bodies. This is tantamount to providing a "search engine" service for police. As explained in the consultation document: "*The police (may want to) find offenders more efficiently than is currently the case… (and could) use the NFI data matching to help locate a person's address or employment details as part of their criminal investigations. This would be seen as a part of their intelligence gathering processes."*

"*The NFI offers police forces a more effective way of searching locally held records from multiple organisations simultaneously. Currently, individual requests are made to separate local authorities/government departments using written data protection exemption requests."*

Chris Pounder, a specialist in information law, has explained that this means the Cabinet Office "brazenly calls for the undermining of fundamental protections for data subjects" because these data protection exemption requests contain a balancing exercise where the rights of the person involved, including to know whether their data has been shared,[11] are curtailed on an

---

[9] https://royalsociety.org/-/media/policy/Publications/2021/learning-data-lessons-data-access-and-sharing-during-COVID-19.pdf?la=en-GB&hash=DA87DF3B44154E407FDADC6B4269CEED

[10] https://techcrunch.com/2020/09/09/uk-wants-pandemic-levels-of-data-sharing-to-be-the-new-normal/

[11] (Schedule 2, Para 2(1) of the DPA 2018)

exceptional basis for dealing with crime. The proposed “more effective” mechanism would tip that balance unfairly in favour of the police.

Private sector identity service

Over the past decade there have been many debates over the creation of identity regimes in the UK, from the failed introduction of ID cards to the Verify system. The proposals appear to side line these debates by creating a system where private organisations can buy access to the NFI tools, now expanded to a broad range of purposes, including correcting errors in datasets. Credit reference agencies are only one of the sectors involved, but there is not statutory limit on who can be given access, which is under the discretion of the Cabinet Office, and with an economic incentive to earn more fees.

As Chris Pounder explains: ’For a few thousand pounds, such employers can demonstrate to the immigration authorities that they have expended every effort not to employ persons who cannot work in the UK.”

This kind of development requires extensive debate and should not be introduced through a statuary instrument with a few weeks’ notice.

Data rights and privacy

The proposals do not provide sufficient safeguards to protect the right to privacy.

As Chris Pounder explains, the consultation conflates mandatory and voluntary data sharing, but the data protection regime is very different in those cases. For example, there is a right to opt-out of voluntary sharing, which is not explained or discussed anywhere in the consultation document or any other NFI privacy documents.

The responsibilities of the Cabinet Office vs the participant organisations are not clearly defined, making it more difficult for individuals to exercise their rights.

More importantly, mandatory data sharing will involve several exemptions to the subject rights:

“*2.16.3.Individuals’ subject access rights may be limited as a consequence of exemptions from data protection legislation. This determination should be made on a case by case basis by the organisation in receipt of the request for information. This means that individuals may, in some cases, be refused full access to information about them that has been processed in data matching exercises.”*

Pounder explains that because the regime “can negate most of the data subject rights as well as well as the first two Principles in Article 5 (GDPR)… compliance with the UK’s data protection regime is touted in the consultation documents as a safeguard, when it is not.” This means that ”the main safeguard is Article 8 of the Human Rights Act, yet any analysis of Article 8 is absent from the Government’s consultation text or Draft Code.”

Stigmatisation and dignity

These new mandatory powers for dealing with errors are a huge expansion of state data-sharing that requires a much broader debate. This is a form of automated profiling, which is recognised in data protection law to carry higher risks. While fixing errors may seem a good reason for sharing data this can have negative consequences and be perceived as intrusive, and even when it is for delivering benefits to those who are entitled there are problems with stigmatisation.

ORG was part of a policy process to increase data sharing in the Digital Economy Act 2016, and these concerns came up repeatedly. For example, in the sharing of data about free school meals, where stigma was one of the main reasons for lower uptake. The consultation document mentions free school meals again, despite NFI staff being present in those discussions. The need to respect the dignity of those involved, who had the right to avoid benefits if they wanted, was extensively discussed with the Cabinet Office.

ORG's basic principles at the time were:

"ORG's minimal criteria are that data sharing agreements should not lead to a widespread intrusion on people's privacy; should be proportionate, limited in scope and enshrine fundamental rights; and carry strong safeguards against wilful abuse and unintended consequences."[12]

Debt and COVID

The government is already openly advocating to create new powers to deal with the expected levels of debt owed to government caused by the COVID-19 pandemic "due to COVID fiscal stimulus packages and other emergency response measures (…) and increasing the number of vulnerable people interacting with government debt recovery processes."

The proposals focus on being able to trace individuals with outstanding overdue debt and fast track the recovery, but also mention possibly helping people manage their debt. These discussions about debt fairness already took place at the time that the Digital Economy Act was passed and the Cabinet Office admitted that they were wishful thinking because there was no mechanism for government departments to coordinate.

Unclear data retention practices

Chris Pounder has raised issues with the data retention schedules, which in the current proposals are reduced to three months after the matching exercise. However, as Pounder explains, the NFI could have access to the data for a longer time if the matching period is included. Besides, retaining data after a negative match (the majority of cases) is "contrary to any basic data protection analysis".

Additionally, providing an ongoing data matching service as described in the documents would require permanent access to some large critical databases, which means that in practice the published schedules for data deletion could mean permanent rolling requests. The government should clarify whether retention schedule rather means update intervals.

Lack of consultation

A review of Hansard shows that there was a limited discussion of these expansive powers but some concerns were raised:

"*It should be stressed that neither the further purposes described nor the additional one arising from this amendment can be a proper purpose of data matching until introduced by regulation following wide consultation. (Lord McKenzie of Luton)"*[13]

---

[12] http://www.openrightsgroup.org/publications/orgs-response-to-data-sharing-consultation

[13] http://hansard.parliament.uk/lords/2013-06-26/debates/13062667000086/localauditandaccountabilitybill(hl)?highlight=local%20audit%20accountability%20act#contribution-holothdt2013062667000086SCBK-Bntgamendmentod187

While the Cabinet Office has consulted extensively within government, there has been almost no consultation with citizens or civil society. The new powers were uncovered by Chris Pounder, who raised the alarm.[14]

Have your say

You can have your say by responding to the Government's consultation.

[14] https://amberhawk.typepad.com/amberhawk/2021/02/the-return-of-the-database-state-mandatory-data-matching-and-expansive-data-sharing.html