Consultation

A. The NFI should widen the data matching powers to include prevention and detection of crime (other than fraud).

strongly disagree

The expansion of the already extensive data-sharing powers of the Cabinet Office powers to the “prevention and detection of crime” is likely a disproportionate intrusion on fundamental rights. The personal data of millions of people in the UK is already shared and justifying the current regime would already require strong restrictions, which the narrower focus on fraud just about provides. Expanding this system into a generalised monitoring of large numbers of the population for undefined crime prevention would likely fail a proportionality test.

A non-exhaustive list of problems to be examined would include:

- the generalised nature of the data collection across the population. The NFI currently collects more than 20 data types, over 8000 datasets, which is over 300 million data records from 1300 participant organisations;
- there is no opt-out of mandatory data sharing and people cannot avoid engaging with the public sector in their dealings so this is akin to monitoring public spaces;
- the objective is not narrowed to more serious crimes;
- the data analytics techniques can becomes increasingly sophisticated so it is hard to predict and foresee the intrusion;
- the nature of data matching is creating new potential suspects of crime. In principle, this is just a flag, but there is evidence from other fields that automated decisions bias human supervision, so the initial matching could have a larger impact than expected.

In addition, it is likely that this extension will affect vulnerable groups. Migrants in particular could be affected because of the ongoing policy formerly known as the “hostile environment”. This means that the Home Office will attempt to use any minor issue to take away any entitlements with the aim to make life in the country unpleasant and difficult so they choose to leave the UK. The existing data sharing already involves checks on migration status and sharing of data with the Home

Office. Hundreds of Tier 1 highly skilled migrants have been denied indefinite leave to remain (ILR) after being accused of deceptive behaviour due to minor tax discrepancies and clerical errors,[1] under paragraph 322(5) of the immigration rules.[2] According to immigration specialist lawyers, these cases are "are amongst the most challenging to win".[3] 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.

The police have long argued that their involvement in immigration matters has a detrimental impact on policing and community relations. So although immigration offences such as overstaying visas and illegal entry were criminalised by the 1971 Immigration Act, they were rarely enforced by the police, reflected by extremely low prosecution and conviction rates. In 2012, however, a new 'joint working operation' between the police and Home Office codenamed Operation Nexus was piloted in London, before being rolled-out nationally. The details vary by region, but typically include having immigration officials embedded at police stations, police officers checking people's immigration status, and police contact and intelligence used to build deportation cases.[4]

B. The NFI should widen the data matching powers to include apprehension and prosecution of offenders.

strongly disagree

The prosecution of offenders presents distinct issues to the general prevention of crime. In this case the data matching is more targeted than in the former case as there is already a basis for suspicion, which for now we can assume would be based on separate evidence. We are nevertheless concerned about the apparent lack of safeguards.

Expanding the capacity of police to collate information from public and private bodies in the way it is proposed 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

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

[2] https://www.gov.uk/guidance/immigration-rules

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

[4] (Griffiths, 2017; Parmar, 2019). https://journals.sagepub.com/doi/full/10.1177/0261018320980653

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."

This last paragraph betrays a disregard for the current systems of checks and balances that aims to protect human rights.

According to data protection expert Chris Pounder[5] this means the Cabinet Office "brazenly calls for the undermining of fundamental protections for data subjects". The data protection exemption requests that the police find so cumbersome contain a balancing exercise where the human rights of the person involved, including the data protection right to know whether their data has been shared,[6] are curtailed on an exceptional basis for dealing with crime. The proposed "more effective" mechanism would turn the current system on its head from exceptional access to routine. This would be open to legal challenges.

The proposed system does not even appear to include any controls to ensure that the police would not abuse their new capacity to trawl databases.

C. The NFI should widen the data matching powers to include prevention and detection of errors and inaccuracies.

strongly disagree

The principle that organisations should maintain data quality is important, but this cannot be justified to increase the processing of data in a way that generates new insights. Unfortunately, this seems to be the case here, as we cannot separate the fixing of errors from the use of the data for the other purposes.

In principle, expanding the powers to fixing errors and inaccuracies without the other new proposed powers on crime and debt would appear to be less intrusive and raise fewer concerns. However, there are many issues that make this proposal

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

[6] (Schedule 2, Para 2(1) of the DPA2018)

problematic in its own terms.

If the aim was simply to fix minor errors, such as misspelt names or addresses or maiden and married name confusion, this may be more justified and most people would find this useful, but the proposals will change the *entitlement status* to various public services. This is a completely different activity that cannot be justified simply under the guise of *data quality.*

There is a lack of due process throughout this exercise, where any matching for error fixing could trigger all kinds of unpredictable consequences. Discrepancies and anomalies could be interpreted as evidence of wrongdoing, which could lead to authorities cutting off support for groups already vulnerable and marginalised who will find it even harder to seek redress and in the meantime have no means of support. The NFI focuses on data matching, that is comparing datasets looking for inconsistencies. If these are discovered, it is the responsibility of the organisations involved to follow up and find if there is actual fraud or some other issue. As the administrative decision is carried out by a separate organisation from the NFI, the process to challenge the decisions could become more difficult for people affected.

As with crime, currently the proposals for errors and inaccuracies do not provide comprehensive institutional safeguards for the handling of personal data, for example mandatory notifications to the people affected by error identification before they see any change in their entitlements. In this case it would be hard to see why the principle of transparency in data protection would be exempted. Data matching in any context faces some serious problems of reliability and the potential creation of new errors.

Furthermore, taking the data out of context by a unit at the Cabinet Office removed from the direct provision of services makes it harder to make nuanced interpretations. The kind of information we are dealing with here is highly intimate and potentially complex, for example the relationships of cohabiting couples or families with multiple parents. This is particularly problematic for vulnerable and marginalised groups[7].

The use of private sector data adds a problematic dimension that gets uncomfortably close to a national ID system by stealth. 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 by the last Labour government to the Verify system. The current proposals appear to sideline 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.

This will have wider consequences, for example in the migration context. As Chris Pounder explains: “For a few thousand pounds, such employers can demonstrate to the immigration authorities that they have expended every effort not

[7] Automating inequality Virginia Eubanks

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. These new mandatory powers for dealing with errors are a huge expansion of state data-sharing that require a much broader debate.

This data matching 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 years ago. 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."[8]

D. The NFI should widen the data matching powers to include recovery of debt owing to public bodies.

strongly disagree

The consultation documents partly justify the creation of these new powers in order 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 extension of data matching powers to assist in the recovery of debt owed to public bodies may not be appropriate when the inequalities present before the

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

pandemic have both increased and widened. The Citizens Advice Bureau has described the situation as a ‘burgeoning debt crisis.’ With one in four UK adults at financial risk, the number of data records involved is likely to increase exponentially. Migrants in particular are facing desperate situations leaving some with little to no income. In a letter to Sir Patrick Vallance earlier this year, the Joint Council for the Welfare of Immigrants wrote that:

> *‘the majority of migrants in the UK have ‘No Recourse to Public Funds’ and that ‘long before the pandemic, NPRF restrictions have been pushing working families into abject poverty, forcing them into unsustainable debt … Since the Covid-19 outbreak, this situation has considerably worsened.’*

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 2017. The DEA contained various safeguards to provide some control over the use of these powers, which were piloted on the basis of a clear business case, data impact assessments, and a statement on how the departments using the data would comply with the Fairness Principles[9] developed partly as a result of ORG’s mobilisation of debt management groups in the DEA policy making process. It is unclear how these new powers will be applied.

Before any new powers are created, the public needs to know more about how the existing powers are already used. When the DEA was being drafted the Cabinet Office admitted that the practical impact of data sharing on public debt would be limited because there was no mechanism for government departments to coordinate and prioritise multiple debts. To deal with this issue, the government created the Debt Market Integrator as a semi-private joint venture with Equifax. The new company Indesser states that they have recovered over £2 billion in public sector debt for 17 government bodies, using “data, analytics and the resulting insight to enhance understanding of customers who owe money, and then define and implement fair and effective treatment strategies based on their individual circumstances”.[10]

The Cabinet Office has also developed a Debt Management Function and consulted on consulted on this complex issue[11], where any reforms should be part of a wider change to the machinery of government. There is widespread agreement that debt management in the public sector can be improved,[12] but the creation of new data matching powers without additional mechanisms to increase fairness could do more harm than good.

[9] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/799335/FairnessGroupJointPublicStatement_20190502.pdf

[10] https://www.indesser.com/

[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/895296/Fairness_in_gov_debt_management_Call_for_evidence_WEB.pdf

[12] https://commonslibrary.parliament.uk/research-briefings/cbp-9007/

Do you want to raise any particular equality related issues in relation to this proposal?

As data matching is a type of large-scale profiling of individuals with legal effects and ‘likely to result in high risk’ it has the potential to be harmful to migrant communities therefore careful attention needs to be applied and continuous monitoring carried out – privacy, safety and discrimination concerns.

As we discussed above, we are concerned about the impact that the proposed measures are likely to have on vulnerable groups specifically migrants. Examples of the data matches the NFI already does include several migration examples.

- An employee is working for one organisation while being on long-term sick leave at another
- Failing to declare an income while claiming housing benefit.
- Payroll records to records of failed asylum seekers.
- Obtaining employment while not entitled to work in the UK.
- Claiming housing benefit despite having a housing tenancy elsewhere.

The increasing sharing of personal data and associated data process could result in discrimination against certain groups or individuals in the way that their personal data was used. There is reason to believe that growing data matching for immigration purposes is likely to occur as the Government’s Hostile Environment becomes increasingly digitised.

Do you have any views on the updates to the Code of Data Matching Practice?

The Code of Data Matching Practice is deficient, particularly in not making clear who is the data controller when mandatory data sharing powers are used by the Cabinet Office. The Code says that in most cases the participant organisations will be data controllers, but in our view in most cases of mandatory data sharing the Cabinet Office will at least have joint if not full controllership.

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

Confusing data governance and weaker subject rights

As discussed above, the responsibilities of the Cabinet Office vs the participant organisations are not clearly defined, making it more difficult for individuals to exercise their rights or access, correction, etc.

The consultation conflates mandatory and voluntary data sharing, but the data protection regime is very different in those cases.

Consent, trust and the right to object

This confusion over the legal bases for data sharing is particularly important with relation to the right to object to data sharing that is not mandated by law, which is not explained or discussed anywhere in the consultation document. The NFI Privacy Policy explains this:

"Where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller: You have the right to object to the processing of your personal data. This right does not apply where your data is disclosed to us under a legal obligation under Paragraph 2 of Schedule 9 of the Local Audit and Accountability Act 2014."[13]

However, as we discuss below, data exemptions may apply in some cases and individuals may not know in which cases they can object and when not.

The recent report on *Addressing trust in public sector data use* by the UK Government Centre for Data Ethics and Innovation sets out that:

"The sharing of personal data must be conducted in a way that is trustworthy, aligned with society's values and people's expectations. Public consent is crucial to the long term sustainability of data sharing activity."[14]

The NFI Privacy Notice makes it clear that data processed under the Local Audit and Accountability Act 2014 does not require consent. While the technical consent under data protection may not apply to much of the data processing of the NFI, the general principle of public consent surely should be retained.

The proposals do not protect the fundamental right to privacy

[13] https://www.gov.uk/government/publications/fair-processing-national-fraud-initiative/fair-processing-level-3-full-text

[14] https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use

Some data sharing will involve several exemptions to data 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.”

Chris 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.”

A human rights analysis should make a clear case for the necessity of the powers and data sharing to comply with a legal obligation and what less intrusive alternatives would may available, which is absent from the consultation.

Excessive retention periods and ongoing rolling databases

Mr Pounder has also raised issues with the data retention schedules, which in the current proposals are reduced to three months after the matching exercise. However, as he 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 to a dataset that will be permanently accessible.

Other issues

The expansion of these powers deserves proper parliamentary scrutiny and wider consultation

These new powers were buried as optional measures in the Local Audit and Accountability Act 2014,[15] but the Government has chosen to activate them now, we can only assume in connection somehow to the new National Data Strategy. Government data policy was moved back to the Cabinet Office from DCMS in July 2020.

The powers are introduced by ministers through secondary legislation in an affirmative statutory instrument (SI) and both Houses of Parliament have to approve them. This process raises important questions of democratic accountability as the 2014 Act was not broadly discussed in these terms of creating a huge law enforcement data matching power across the whole public sector.

The 2014 Act was presented at the time by the government as an exercise in local democracy and there was no detailed discussion of these powers. The focus of the Act was on dismantling the Audit Commission and creating local accountability systems. In their explanatory documents[16], the government mentioned in passing that some of the previous powers of the Audit Commission under the Serious Crime Act 2007[17] would pass to the NFI.

A review of Hansard[18] shows that there was a limited discussion of these expansive powers but some concerns were raised. A huge amount of data sharing was taking place at the Audit Commission, but at that time this was restricted to fraud and mainly local authorities, and not to broader law enforcement. Nevertheless, the existing powers of the Audit Commission at the time, inherited by the Cabinet Office, were acknowledged to be quite excessive, even by Government ministers:

"I must say that I had not appreciated how extensive data sharing was within the Audit Commission and local government. Central government has been approaching this matter with a rather greater degree of caution and hesitation. Perhaps I should phone the Guardian and tell it just what the Audit Commission has been doing in this regard. I am sure that that newspaper would like to make it a front-page spread. (Lord Wallace of Saltaire, Minister for the Cabinet Office at the time 2013-14)"[19]

"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

[15] https://www.legislation.gov.uk/ukpga/2014/2/schedule/9

[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/198057/Local_Audit_and_Accountability_Bill_-_plain_English_guide.pdf

[17] https://www.legislation.gov.uk/ukpga/2007/27/part/3/chapter/1

[18] Ibíd.

[19] https://hansard.parliament.uk/search/Statements?searchTerm=Local%20Audit%20and%20Accountability%20Act&startDate=01%2F01%2F2013%2000%3A00%3A00&endDate=12%2F01%2F2014%2000%3A00%3A00

of Luton)"[20]

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 data protection expert Chris Pounder, who raised the alarm.[21]

The operation of LAAA 2014 powers together with the Digital Economy Act 2017 causes legal uncertainty

The Digital Economy Act 2017 (DEA 2017) introduced new powers for data sharing across government for several specific purposes that included dealing with fraud and debt owed to public bodies. The DEA has no powers related to the crime, offenders, or error and inaccuracies and excludes the NHS. The DEA included other powers for data sharing for improving public service delivery, research and civil registration. All powers in the DEA are permissive and not mandatory as in the 2014 Act.

ORG participated in extensive consultations with the Cabinet Office to introduce safeguards in the data-sharing powers in the DEA[22] 2017. Partly through ORG's pressure, the powers for fraud and debt in the DEA were introduced on a pilot basis that required explicit renewal to continue.

The powers have been used for several pilots, but there is little discussion about their success. These include for example using driver's licence data of Universal Credit claimants to identify possible other adults at the same address revealing a risk of undeclared partner fraud, and sharing data of HMRC and Student Loans to look for childcare costs claims.[23]

Before new powers are introduced we need to improve the use of existing powers.

The DEA powers were expected to streamline data sharing and bring more transparency. There are registers for data sharing under the powers.[24] but more broadly transparency on sharing is limited. Many of the pilots relate to council tax debt collection.

The NFI consultation document explains that the two regimes under the DEA and the 2014 Act are used at the same time:

[20] https://hansard.parliament.uk/Lords/2013-06-26/debates/13062667000086/LocalAuditAndAccountabilityBill(HL)?highlight=local%20audit%20accountability%20act#contribution-HOLOTHDT20130626DB13062667000086SCBK-Bntgamendmentod187

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

[22] https://www.openrightsgroup.org/blog/update-on-data-sharing-policy-process/

[23] https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/mid-point-report-on-use-of-the-dea-powers#updates-on-use-of-the-information-sharing-powers

[24]{$NOTE_LABEL} https://registers.culture.gov.uk/

“17.5.There are instances, however, where both the 2014 Act and the DEA have been used side by side within the CO. For example, NFI used the 2014 Act to provide data to HMRC; HMRC then added data and provided back to the NFI using the DEA. Data matches were then available to NFI participants using the 2014 Act.”

This practice raises serious concerns and should be explained in detail.

The funding model of the NFI causes an incentive to share data

The consultation document explains that the NFI expect that new databases and organisations will be added to the programme if the new powers are enacted.

The NFI charges each participant between £1,000 and 5,000 and it covers most of its £2.4m budget from these fees. This creates an incentive to increase data sharing.

The NFI carries out regular large scale data matching exercises but in addition provides several web-based services to private and public organisations:

ReCheck: organisations can repeat data matching exercises at a time that suits them.

AppCheck: help verify people’s identity or if they have left out relevant information that might affect their entitlement to a benefit, service or employment.

FraudHub: participant bodies can pool their data in order to prevent errors in processing payments and to reduce fraud.

These services expanded to the new powers could see a huge expansion of private sector participant organisations.