Privacy International's response to the National Fraud Initiative Consultation

March 2020

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

Answer: Strongly disagree.

The proposed expansion of the NFI into general crime, and into the apprehension and prosecution of offenders, raises three important problems.

Firstly, it does not clarify which law enforcement agencies will be able to use the NFI for data-matching for the purposes of the prevention and detection of crime. While the Consultation document mentions that the police "may want to use the NFI data matching to help locate a person's address or employment details", it does not provide any guarantees that this prerogative will only be exercisable by the police. If intelligence agencies are to have access to the NFI, the Draft Code should make this clear and outline their powers and responsibilities. Without sufficient safeguards and oversight in place, providing access to a broad range of users and agencies can lead to misuse and exploitation of personal data made available on the NFI. Even if access were to be extended only to the police, significant data protection concerns remain. The police already have access to a significant amount of data through the Police National Database and the Police National Computer, which is set to expand through the proposed Law Enforcement Data Service (LEDS). Being allowed to access data through the NFI is likely to add to the already vast trove of information at the police's disposal. The fact that this purpose is intended to inform "intelligence gathering processes" is far from reassuring. The nature of intelligence material is such that it is very unlikely to ever be subject to scrutiny or challenged.

Secondly, while the proposed updates to the current framework set a defined number of additional purposes for the data-matching exercise, they do not meaningfully qualify the purposes for which a single participant to the NFI may use the data-matching exercise. There is nothing to suggest that the use of the NFI for the purpose of preventing and detecting crime will be exclusively limited to law enforcement. This means that, in theory, a participating body which does not exercise law enforcement functions may nonetheless use the NFI for crime detection/prevention purposes. For example, nothing would prevent an employer from running the data-matching exercise to obtain information that is not strictly relevant or necessary to their employment relationship with the employee, but could nonetheless inform the employer's perception of the employee and potentially impact their assessment of his/her performance. Thirdly, while access to the NFI data-matching exercise is made conditional upon payment of a fee, once a public/private sector organisation purchases access to the NFI, the cost of individual searches becomes nominal. If using AppCheck, participating entities pay £1.10 per search for their first 250 searches; if the number of searches is higher, the price per search decreases even more.[1] Therefore, there is no real financial deterrent for participating entities from carrying out NFI data-matching checks for a large number of individuals.

Further, it is likely that some of the equality-related issues in the criminal justice sphere will be replicated in the implementation of the proposed changes to the NFI.

Multiple indicators show that police powers in England and Wales are used disproportionately against black, Asian and minority ethnic (BAME) people. The figures for 2019-20 show that black people are nine times more likely to be stopped and searched by police than white people; BAME individuals were overall 4.1 times more likely to be stopped and searched than those from a white ethnic group.[2] Racial bias in policing has continued unabated during the pandemic. In 2020, figures published by the National Police Chiefs' Council ("NPCC") found that the police in England and Wales were twice as likely to fines for breaches of the Coronavirus regulations against young BAME men (aged between 18 and 34) than white men of the same age.[3] While incurring a fine is not of itself a crime, failure to pay the fine within 28 days results in the fine being registered with the court, meaning that the court is empowered to enforce the fine and potentially issuing a warrant for arrest if a person fails to respond.

This is unsatisfactory both from a data protection and equalities standpoint. Concerns relating to the disproportionate impact of data processing on minority communities are not new. The Information Commissioner's Office (ICO) has previously found that the Police contravened data protection principles in its

[1] Cabinet Office/NFI, National Fraud Initiative 2020/21: Mandatory and Voluntary Public Sector Fees. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910298/Mandatory-and-Voluntary-Public-Sector-Fees-NFI-2020-21.pdf; Cabinet Office/NFI, National Fraud Initiative 2020/21: Private Sector and Non-Public Sector Voluntary Participant Fees. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910234/Non-Public-Sector-and-Private-Sector-Voluntary-fees-NFI-20-21.pdf

[2] Home Office, *Police powers and procedures: England and Wales*, year ending 31 March 2020, second edition. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/935355/police-powers-procedures-mar20-hosb3120.pdf

[3] National Police Chiefs' Council, *Policing the Pandemic: Detailed analysis on police enforcement of Health Regulations and an assessment of disproportionality across ethnic groups*, July 2020. Available at: https://news.npcc.police.uk/resources/policing-the-pandemic-4

investigation into the Gangs Matrix,[4] and Mobile Phone Extraction.[5] In particular, the ICO had significant concerns regarding the data entered into the Gangs Matrix database. Statistics from July 2016 show that 87% of the people recorded in the Gangs Matrix were from Black, Asian or Minority Ethnic (BAME) backgrounds. Further, 78% were Black, despite the fact that only 13% of London's total population are Black. Additionally, 99% of people recorded on the Gangs Matrix were male.[6] PI has previously raised these issues in its response to the College of Policing's consultation on the Law Enforcement Data Service (LEDS).[7]

There is nothing to prevent the new iteration of the NFI from reproducing the racial bias which permeates other aspects of the criminal justice system.

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

Answer: Strongly disagree.

The proposed expansion of the NFI to detect errors and inaccuracies is extremely concerning, as it amounts to an open license to run the data-matching exercise to spot inconsistencies, many of which will surely be clerical errors of little consequence. This means that participants to the NFI will be able to legitimately run the data-matching exercise needing next to no justification, and easily launch into fishing expeditions targeting beneficiaries. This approach directly contravenes the principle of data minimisation, raising significant data protection risks and begging the question whether open-ended access to the data contained in likely to be relevant, adequate and necessary. This is similarly concerning from a human rights standpoint, where concerns of proportionality become significant.

On the Consultation paper, the introduction of the new power to prevent and detect errors and inaccuracies is justified on account of its potential to help local authorities "to ensure citizens get access to their full benefit entitlements". However, research ostensibly suggests that benefits underpayments are not caused by data errors in as much as they are caused by the fact that benefits claimants are provided with little information about how their costs are calculated. A seminal report by the Child Poverty Action Group (CPAG) found that the lack of information made it difficult for Universal Credit claimants to see if they were being

[4] Information Commissioner, *Enforcement notice addressed to the Commissioner of Police of the Metropolis*. Available at : https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf

[5] ICO, *Mobile phone data extraction by police forces in England and Wales*, June 2020. Available at: https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

[6] Information Commissioner, *Enforcement notice addressed to the Commissioner of Police of the Metropolis*. Available at : https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260336/metropolitan-police-service-20181113.pdf.

[7] Privacy International, *Challenging over-policing: our response to the public consultation on the Law Enforcement Data Service (LEDS),* 3 September 2020. Available at: https://privacyinternational.org/news-analysis/4154/challenging-over-policing-our-response-public-consultation-law-enforcement-data

underpaid; a problem that could be easily fixed if the various elements of the award were clearly separated and accounted for in the information provided to the claimant.[8] In many of the cases reported by CPAG, beneficiaries were largely unaware of underpayments until they sought the help of experienced welfare advisers. The most helpful solution, therefore, is not to increase "backdoor" data-matching to ensure that data held is accurate; instead, beneficiaries should be provided with more detailed information enabling them to flag and correct any mistakes.

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

Answer: Strongly disagree.

PI is concerned that this new purpose may lead to the policing of the poor, and may disproportionately impact minority communities.

Despite this, PI has documented the use of novel techniques by public bodies to recover debt owed to them. Last year, our research revealed that local authorities used social media monitoring for debt recovery purposes.[9] Expanding the NFI to include debt recovery will vastly increase the significant data already available to local authorities, and potentially the data that is accessible to debt collection agencies used by local government.[10] It is currently unclear whether the data accessed by local authorities through the NFI will be subsequently passed on to debt collection agencies.

The financial and socio-economic impacts of the pandemic have been felt differently across ethnic groups, with the BAME community bearing the brunt of job cuts during the pandemic. An analysis published by the Trades Union Congress[11] in January 2021 found that BAME workers had been hit much harder by job losses during the pandemic than white workers, with the number of BAME in employment dropping by 26 times more than the drop of white workers over the same period. Similarly, an IPPR analysis of the *Understanding Society COVID-19 Study*,[12] a longitudinal survey of UK households during the pandemic, found that BAME groups were more likely to be renters – limiting their scope to reduce costs in the face of

[8] CPAG, Computer Says 'No!'. May 2019, pp. 12-13. Available at: https://cpag.org.uk/sites/default/files/files/policypost/Computer%20says%20%27no%21%27%20Stage%20one%20-%20information%20provision.pdf

[9] Privacy International, *The use of social media monitoring by local authorities – who is a target?*, 24 May 2020. Available at: https://privacyinternational.org/explainer/3587/use-social-media-monitoring-local-authorities-who-target

[10] Owen Walker, *Local councils criticised for 'concerning' debt collection tactics*, Financial Times, 27 April 2020. Available at: https://www.ft.com/content/06689a51-2351-49f1-a5f6-1f97a4024243

[11] TUC, *Jobs and Recession Monitor – BME workers*, 20 January 2021. Available at: https://www.tuc.org.uk/research-analysis/reports/jobs-and-recession-monitor-bme-workers

[12] University of Essex, Institute for Social and Economic Research, Understanding Society: COVID-19 Study, 2020. 7th Edition. UK Data Service. Available at: https://beta.ukdataservice.ac.uk/datacatalogue/studies/study?id=8644

an income shock – and that they felt they were at greater risk of falling into arrears due to the pandemic.[13]

These studies suggest that ethnic minority groups are more likely to incur debt during the pandemic. Consequently, any data-matching exercise run for a debt recovery purpose is likely to disproportionately affect BAME groups.

In addition to BAME individuals, single-parent families may also be particularly affected by any data-matching exercise carried out in the name of debt recovery. A recent report found that single parents disproportionately experience problem debt and were particularly affected by the pandemic, with half of the parents surveyed reporting that they had taken on more debt since COVID-19.[14]

E. <u>Do you want to raise any particular equality related issues in relation to this proposal?</u>

In addition to the concerns highlighted above, PI notes that the proposed expansions, in particular in relation to the prevention and investigation of general crime, may disproportionately affect individuals of the BAME community in the enforcement of immigration offences. The 2015 NFI public sector case studies[15] provide a few examples of the successful detection of individuals having fraudulently claimed to have right to work in the UK. If the proposed expansion into general crime were to take place, the NFI data-matching capabilities could be called upon to investigate the wide range of existing immigration offences, including illegal entry and overstaying. Considering that an undisclosed number of private actors can have access to the NFI on a voluntary basis, it is likely that many private entities will seek to access data made available to them by the NFI data-matching exercise.

PI has identified at least two groups of private actors whose use of the data-matching exercise raises particular concerns.

a) Landlords

In 2019, the High Court ruled that the Right to Rent scheme introduced by the Immigration Act 2019, led to nationality and race discrimination against individuals who had the right to rent but did not have British passports.[16] The scheme prohibited landlords from renting properties to people from outside Europe without

[13] IPPR, Black, Asian and minority ethnic groups at greater risk of problem debt since Covid-19. Available at: https://www.ippr.org/blog/minority-ethnic-groups-face-greater-problem-debt-risk-since-covid-19

[14] Gingerbread, The single parent debt trap, February 2021. Available at: https://www.gingerbread.org.uk/policy-campaigns/publications-index/the-single-parent-debt-trap/

[15] Cabinet Office, NFI: public sector case studies, March 2015. Available at: https://www.gov.uk/government/publications/national-fraud-initiative-case-studies/nfi-public-sector-case-studies#immigration

[16] *R (Joint Council for the Welfare of Immigrants) v SSHD* [2019] EWHC 452 (Admin).

leave to remain in the UK. This finding was upheld by the Court of Appeal.[17] In light of this example, one may reasonably expect that, if given the opportunity to do so, private actors may choose to run the NFI data-matching exercise against prospective tenants without a British passport.
Robust safeguards are necessary to ensure that similar instances of discrimination arise do not arise from the use of the NFI data-matching capabilities by private actors.

b) Employers

The 2015 NFI case studies show two examples of NHS Trusts' employees being flagged by the data-matching exercise (payroll information as assessed against UK visa immigration datasets) as having fraudulently declared that they had the right to work in the UK. At the time these case studies were developed, the NFI data-matching exercise could only be run for the prevention and detection of fraud. As such, the information that public sector employers listed as mandatory participants to the NFI (i.e. listed in Schedule 9 to the Local Audit and Accountability 2014 Act) could lawfully obtain from the data-matching exercise was largely limited to verifying whether they had been given true or false information in relation to an essential job specification. The proposed expansion to the NFI vastly increases the information that can be accessed by employers.

The increased data-matching capabilities of the NFI and the opportunities they present for employers must be understood in light of current legislation and the obligations it imposes on employers. Employers commit a civil offence when they "knowingly" employ an undocumented person, or have "reasonable cause to believe that the employee is disqualified from employment by reason of the employees' immigration status". It is possible that employers will make use of the NFI data-matching exercise in order to protect themselves from liability, and use the NFI as an additional layer of right to work checks. If so, there is a real risk that BAME and/or non-British prospective employees will be disproportionately subjected to these checks. This issue is compounded by the lack of transparency, which we detail in section G below.

PI has not seen any safeguards which could prevent private parties participating in the NFI accessing information which is not strictly relevant, necessary and adequate. Neither the Consultation nor the Draft Code explain how the Cabinet Office will ensure that relevant data protection rights and principles are protected. There is similarly no information on how, if at all, the NFI will seek to mitigate disproportionate adverse impacts on minority communities.

At a minimum, the Draft Code should outline robust controls as to how participants to the NFI access information, and meaningful limits to the types and categories of information that they can access. The Draft Code should similarly clarify if any differences exist in the types, categories and granularity of information that can be accessed by mandatory and voluntary participants. If no such differences exist i.e. the level of access provided to both mandatory and voluntary participants is

[17] *SSHD v R (Joint Council for the Welfare of Immigrants)* [2020] EWCA Civ 542.

the same, further guarantees are necessary to ensure that data subjects are given every opportunity to object.

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

The updates to the Code of Data Matching Practice are too vague to be able to sufficiently assist individuals with managing their information. The Code should be expanded to provide further clarity not merely to organisations participating in the NFI, but society at large and in particular individuals likely to be concerned by any data processing that may take place pursuant to the NFI.

The Draft Code does not once mention profiling, despite the fact that the NFI data-matching exercise falls squarely within the definition of profiling in Art.4(4) of the UK GDPR: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

As the ICO indicates, just because analysis of data finds a correlation doesn't mean that this is significant.[18] As the process can only make an assumption about someone's behaviour or characteristics, there will always be a margin of error and a balancing exercise is needed to weigh up the risks of using the results. This reasoning should be built into the Draft Code.

While the Draft Code states multiple times that no assumptions can be made from any matches, and that no decisions should be made as a result of the data match without having first been considered by an investigator, these statements do not go far enough. The Draft Code should expressly state that the data-matching exercise is a form of automated processing, specifically profiling. Furthermore, the Draft Code should draw attention to Art. 22(1) of the UK GDPR, which establishes that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her. In line with Art.22(1), none of the participating organisations can lawfully make decisions significantly affecting data subjects based solely on data matches resulting from the NFI. It must be made clear that all participating organisations are legally prevented from making significant decisions affecting data subjects based on the NFI under data protection law.

The emphasis on data protection law in paragraph 1.3.2 is welcome. However, the force of this statement is diluted by the fact that the immediately preceding bullet-point states that the 2014 Act "generally removes other restrictions in providing the data to the Cabinet Office". It should be clear that compliance with data

[18] ICO, *What is automated individual decision-making and profiling?* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id1

protection legislation can act as a restriction in providing data to the Cabinet Office. Further, the final bullet-point in paragraph 1.3.2 states that the Cabinet Office *may* report publicly on its data matching activities (emphasis ours). PI recommends that reports on data-matching activities be made compulsory, as well as accessible and understandable to the general public. At a minimum, more detail is required about how reporting will be undertaken and at which intervals. For example. the Draft Code mentions at paragraph 2.6.5 that the Cabinet Office will review the results of each exercise in order to ensure that it is appropriate to continue to match that data. Given that the NFI operates in two-year cycles, paragraph 2.6.5 can be read to mean that the Cabinet Office undertakes a review every 2 years. As such, a potential solution is for the Cabinet Office to make public the results of its internal review taking place every 2 years.

Paragraph 2.6.3 of the Draft Code states that Cabinet Office will undertake new areas of data matching on a pilot basis to test the effectiveness of data matching, and that only matches that demonstrate a "significant level of success in one of the data matching areas should be extended nationally". PI welcomes any approach to data-processing which endorses data minimisation. However, in PI's assessment, the Cabinet Office should clarify what constitutes a "significant level of success". PI refers to its general comments in section G below relating to transparency.

Paragraph 2.10.1 mentions each controller must consider whether a data-matching exercise will trigger a duty to conduct a DPIA. PI endorses this approach, but notes that the Draft Code lacks a similar yet necessary reference to the Cabinet Office's potential duty to conduct a DPIA. It would appear from paragraph 2.8.5 that the Cabinet Office is a data controller for the purposes of the data-matching exercise. This is consistent with the definition of controller in s.4(7) of the UK GDPR, which provides that the controller is the body which alone or jointly determines the purposes and means of the processing of personal data. This is also consistent with paragraphs 2.6.1 -2.6.3 of the Draft Code, which outline the Cabinet Office's mandate to choose datasets to be matched, and to decide whether it is appropriate to accept data from a voluntary participant or to require data from a mandatory participant. Therefore, the Draft Code should be amended to reflect the full extent of responsibilities and duties flowing from the Cabinet Office's decisive power in relation to data processing undertaken under the NFI.

The Draft Code's section on access by individuals to data included in data-matching is similarly lacking in information. Firstly, the section focusses on access rights, and not on the full range of rights available to the data subject. While the exercise of data subject rights in relation to the NFI may be restricted in line with data protection exemptions, and by virtue of the public task processing basis as set out in Art. 6(1)(e), multiple rights remain available to data subjects. For instance, as far as voluntary participants are concerned, data subjects retain the right to object to their data being processed. The Draft Code should at least mention that this right continues to be available to data subjects. Secondly, the section does not sufficiently clarify how responsibilities in addressing data subject requests are split across participating organisations and the Cabinet Office. This lack of clarity could make it difficult for data subjects to exercise their rights, and generate confusion as to which entity to contact.

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

PI strongly believes that the proposed expansion of the NFI raises significant data protection concerns. We look at these concerns in turn through the lenses of the data protection principles enshrined in Article 5 of the UK General Data Protection Regulation (GDPR), and data subject rights.

Data protection principles

(i) Lawfulness, fairness, and transparency

There is currently insufficient information regarding the functioning of the NFI at multiple levels. To start, it is not entirely clear who the data controller is for the data-matching exercise. It would appear from the NFI Privacy Notice and the Code of Practice that the data controller is the Cabinet Office.[19] However, the same Code of Practice suggests that voluntary participants to the NFI are required to provide data in accordance with data protection legislation.[20] The fact that voluntary participants are somewhat responsible for the compliance with data protection obligations – a responsibility which usually attaches to controllers[21] – casts doubt as to who the controller is.

Further, there is limited information as to the functioning of the NFI and its effectiveness. While we are told in the Consultation that in the last two years, the exercise of the NFI identified and prevented fraud, overpayments and errors totalling £245 million. However, we are not told about the following key details:

- The parameters for measuring success for the detection/prevention of fraud purpose, and the suggested future applications which are the subject of the Consultation (e.g., detecting at least 100 instances of fraud per year, or 100 crimes per year);
- The total number of searches carried out so far as part of the NFI data-matching exercise, disaggregated by each participating entity;
- The number of "hits" so far (instances where the data-matching exercise flagged an inconsistency worth pursuing);
- The number of times that a "hit" was accurate;
- The number of times that a "hit" resulted in enforcement action; and
- The number of times that enforcement action was successful.

The above information is fundamental to be in a position to assess whether or not the NFI is effective, and whether or not the data processing is proportionate to the objective sought.

Unclear list of recipients

[19] UK Home Office, Draft Code of Data-Matching Practice, para. 2.8.5. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/959291/Draft_Code_of_Data_Matching_Practice.pdf

[20] Ibid., para. 2.8.4.

[21] GDPR, Art. 24(1).

Similarly, there is little clarity as to the full list of participants to the NFI. While the NFI Consultation paper outlines the datasets matched on a mandatory and voluntary basis, no information is provided as to the entities, both private and public, which participate in the data-matching exercise. While the public sector participants can potentially be gleaned from Schedule 2 to the 2014 Act, the private sector voluntary participants are harder to identify. We know that the list of private entities collaborating with the NFI on a voluntary basis includes housing companies, universities, community rehabilitation companies, charities as well as unspecified private sector participants.[22] However, based on publicly available data, the full extent of participating entities from the private sector is currently unknown. This means that the public and civil society organisations are prevented from knowing the true scale of data processing that will take place as a result of the expansion of the NFI. At a time when the government is promoting further data-sharing through its National Data Strategy,[23] this lack of transparency is particularly concerning, considering that – as shown by the 2015 case-studies published by the Cabinet Office – even the previous, less expansive iteration of the NFI could have a significant impact on the life of an individual.

The fact that a potentially unlimited number of voluntary participants could be having access to data contained by the NFI raises fundamental issues of both transparency and fairness. As outlined above, individuals affiliated to mandatory participants to the NFI do not have the power to object to their data being processed by the NFI and being potentially accessed by thousands of private entities they share no connection with. The government must consider whether it is legitimate or fair for voluntary participants to the NFI to be able to access data that was obtained from the data subjects without their having an opportunity to object. This reinforces the need for the full details of voluntary participants to the NFI to be made public and subject to scrutiny, and for the government to disclose any meaningful limits to the amount and granularity of data accessed by voluntary participants – if any –, or alternatively, an explanation as to why it has failed to distinguish between the levels of access granted to mandatory and voluntary participants.

Missing dataset specifications

Although Schedule 2 to the 2014 Act clarifies that local authorities including county councils, district councils, and London borough councils are mandatory participants to the NFI, the extent of their data contributions to the NFI is unclear. While dataset specifications are provided for housing waiting list data and council tax information – both of which are presumably provided by local authorities – there are no guarantees in the 2014 Act or the Draft Code that the information provided by local authorities will be strictly limited to the categories of data for which public specifications exist. The current wording of the Draft Code simply

[22] Cabinet Office/NFI, National Fraud Initiative 2020/21: Private Sector and Non-Public Sector Voluntary Participant Fees. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910234/Non-Public-Sector-and-Private-Sector-Voluntary-fees-NFI-20-21.pdf

[23] Department for Digital, Culture, Media & Sport, *National Data Strategy*. Available at: https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

states that any guidance containing specifications for each set of data to be included in the data-matching exercise will be made available to participants – not that it will be made available to the public at large.[24] The full specifications – both current and projected – should be made available to the public for inspection and scrutiny.

Further, while the Cabinet Office provides dataset specifications for the NFI across the public sector and private sector, not all datasets listed in Appendix 1 to the Consultation are included. For example, the public sector dataset specification list omits data specifications for DWP State Benefits, Home Office Immigration, and HMRC – all of which are listed in Appendix 1 of the consultation.[25] However, the NFI case-studies make clear that these datasets have successfully been used to detect fraud in the past. No explanation is provided as to why some dataset specifications are omitted.

Department for Work and Pensions

The fact that categories of information shared by the DWP with the NFI are absent from the public domain is of particular concern to PI. In a February 2021 investigation, PI found that the DWP could compel a series of private companies to provide information on beneficiaries, including banks, credit providers, credit reference companies, telecommunications services, educational establishments, and gas, electricity and water companies.[26] Further, PI revealed that DWP officers were encouraged to approach third parties for the purposes of investigating fraud, and were given guidance to undertake physical surveillance.[27] A VICE article covering PI's research told the story of a Personal Independence Payment beneficiary who had been trailed by the DWP at a fundraising event, filmed when exercising, and whose employer and acquaintances had been questioned by the DWP to obtain information.[28]

PI's research indicates that, at least in the case of the DWP, the information that can be given to the NFI is potentially unlimited and may include data obtained through private companies, conversations with third-parties, and multiple instances of physical surveillance. The fact that no data specifications exist for the DWP allows for this obscurity to persist. It is therefore essential that all dataset specifications are made public, so that individuals may know what personal data will be shared as part of the data-matching exercise.

Home Office Immigration

[24] See paras. 2.5.5 – 2.5.6.

[25] Cabinet Office, *National Fraud Initiative: public sector data specifications*. Available at: https://www.gov.uk/guidance/national-fraud-initiative-public-sector-data-specifications

[26] PI, *Shedding light on the DWP Part 1 – We read the UK welfare agency's 995-page guide on conducting surveillance and here are the scariest bits*. Available at: https://privacyinternational.org/long-read/4395/shedding-light-dwp-part-1-we-read-uk-welfare-agencys-995-page-guide-conducting

[27] Ibid.

[28] Josh Gabert-Doyon, How the Government Spies on Welfare Claimants, *VICE*, 2 March 2021. Available at: https://www.vice.com/en/article/y3g9n5/how-the-government-spies-on-welfare-claimants

The fact that the datasets provided by the Home Office are not disclosed is similarly concerning. The immigration exemption in the Data Protection Act 2018 has played and continues to play a significant role in restricting the exercise of data subject rights.[29] In and of itself, this makes transparency in relation to the data provided by the Home Office to the NFI all the more important, necessary, and urgent; particularly when taken alongside recent revelations on the Home Office's data collection activities. For example, PI's research has revealed that asylum-seekers receiving financial support through an ASPEN card were being subjected to surveillance on the basis of their spending habits.[30]

Under data protection law, fairness is intimately linked with an individuals' reasonable expectations as to how their data may be used. Thus, the way data is used as a result of the NFI's expanded powers, and the sources where it may come from, may not be within individuals' reasonable expectations because they are unaware of it or because they are aware of it but find it unacceptable, thus raising questions of fairness. In circumstances where several key aspects of the NFI functioning remain obscure, it cannot be fair for sweeping changes expanding the NFI's capabilities to take place.

All of the missing information outlined in this section should be disclosed as a matter of priority, and in any event before the National Fraud Initiative is implemented.

(ii) Data minimisation

It is doubtful that the amount and granularity of data processed by the data-matching exercise is limited to what is strictly adequate, relevant and necessary.

To start, the founding legislation behind the NFI fails to take proper account of data minimisation. Under Schedule 2, Section 2(1) of the 2014 Act, mandatory participants are obliged to provide the Cabinet Office with the data that may reasonably be required of them. Requiring data to be "reasonable" amounts to a significantly lower threshold than requiring data to be adequate, relevant and necessary. Further, broad phrasing in Section 2(1) leaves the decision-making power largely with the Cabinet Office. One would be hard-pressed to imagine a situation where, when compelled by the Cabinet Office to provide data, a mandatory participant would object on the basis that some of that data was not "reasonably required".

PI's analysis of the documents in the public domain relating to the NFI would also indicate that the NFI, in its current iteration, is inconsistent with data minimisation at large. For example, the NFI does not set a limit on the number of searches a participating entity can run in relation to a specific or multiple individuals. Put differently, a participating organisation can run as many searches as they like, so

[29] Open Rights Group, *The "Immigration Exemption" undermines everyone's data rights*. Available at: https://www.openrightsgroup.org/campaign/immigration-exemption-campaign-page/

[30] Privacy International, *What is an ASPEN card and why does it need reform?,* 23 February 2021. Available at: https://privacyinternational.org/explainer/4425/what-aspen-card-and-why-does-it-need-reform

long as they can afford it. PI also reiterates that, as outlined above, there is nothing compelling participating entities to limit their searches to purposes that are related to their functions. This makes it possible for entities that have no law enforcement functions to take it upon themselves to spot and monitor potential crimes. The data-intensive aspect of the NFI is made apparent in the 2015 NFI case studies, where one immigration-related example casually mentions that a NHS trust, when looking into an employee's right to work in the UK, had come across information about the employee's spouse. The example states that "the employee's wife was also discovered to have no right to reside or work in the UK, but was working for a local employer having deceived that employer who believed she had entitlement to work in the UK". This example shows that participants may choose to carry out NFI searches in relation to individuals with whom they have a tenuous or non-existent connection. The Draft Code fails to explain how this will be discouraged, prevented, or monitored, if at all. It similarly fails to describe how individuals will be protected from any potential misuse of their data stemming from the lack of compartmentalisation or access controls applying to the data processed by the NFI.

(iii) Storage limitation

The Draft Code of Practice states that access to the results of a data-matching exercise on the NFI website will not be possible after a "minimum reasonable period necessary for participants to follow up matches". [31] The Draft Code further states that the Cabinet Office will notify the end date of this period to participants. This indicates a significant degree of discretion and arbitrariness involved in the length of time data-matching results are kept, with the Cabinet Office deciding on a case-by-case basis what the minimum reasonable period is. Strict deadlines for the retention of data-matching results should be implemented to ensure that the principle of storage limitation is enforced.

The Draft Code Practice further states that "all original data transmitted to the Cabinet Office, including data derived or produced from that original data [...] will be destroyed and rendered irrecoverable within three months of the conclusion of the exercise". This directly contradicts the statement reproduced above that data-matching results (i.e. data derived from the original data) will be made accessible "for a minimum period necessary", and causes confusion as to when the three-month period starts running. Indeed it is unclear when the data-matching exercise concludes: does it conclude at the time a match is made on the NFI, or does it conclude when an investigator has ruled that the match is not worth pursuing? The Draft Code is silent on this.

[31] Para. 2.20.2.

Data subject rights

(i) Right to be informed

The Draft Code of Practice states that in line with data protection legislation, NFI participants must inform individuals as to how their data will be processed by way of a privacy notice.[32] The Draft Code similarly suggests that participants may include a link to the Cabinet Office's NFI Privacy Notice. In PI's view, that is not enough. It is possible that several NFI participants will consider that their obligation to inform data subjects is discharged by simply flagging to data subjects that their data may be shared with the Cabinet Office. While this is in theory accurate, the data-matching exercise necessarily entails that the personal data may potentially be shared with all NFI participants. At a minimum, the Code of Practice should require participants (both mandatory and voluntary) to provide the following information to data subjects:

- Clarify that their data may be used for a data-matching exercise;
- Describe all the potential entities with which their data may be shared as part of the data-matching exercise, and for which purposes those entities may access the data subject's data; and
- For each of the NFI powers, provide examples of data matches and the possible interpretations and inferences that can be made from these data matches.

An additional layer of complexity arises out of the current exemptions. For example, the immigration exemption set out in Schedule 2 Part 1 Paragraph 4 of the Data Protection Act 2018 applies to the right to be informed, which can be restricted where its exercise would be likely to prejudice the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the effective maintenance of immigration control. As the 2015 case-studies show, the use of the current iteration of the NFI can have real consequences in the immigration realm. For the reasons explored in the section E above, the proposed expansion into general crime is likely to exponentially increase instances of immigration enforcement through the backdoor. To the extent that the immigration exemption applies, it is unlikely that individuals sharing data with the Home Office will be notified in writing of the Home Office's participation in the NFI – even after the new proposed powers are brought into law.

(ii) Right to object

The NFI Privacy Notice and the Draft Code are clear that data subjects are not in a position to object where personal data is disclosed to the Cabinet Office by a mandatory participant under Schedule 9 of the 2014 Act. In and of itself, this factor is significant enough to warrant a careful assessment of the proposed expansion Cabinet Office's data-matching powers. For each additional power granted to the

[32] UK Home Office, Draft Code of Data-Matching Practice, para. 2.9.1. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/959291/Draft_Code_of_Data_Matching_Practice.pdf

Cabinet Office, more data categories are likely to be requested from mandatory participants. It must be recalled here that the only limit set to the data that can be obtained from mandatory participants to the NFI is that it must be "reasonably required" by the Cabinet Office. A range of new data categories are likely to be seen as "reasonably required" for each of the additional powers.

The position is markedly different with voluntary participants to the NFI. Any data subjects providing data to a voluntary participant are therefore in a position to exercise the full extent of their data rights, including the right to object. However, the NFI Privacy Notice draws insufficient attention to the fact that data subjects may object to the personal data disclosed by voluntary participants to the NFI. The Draft Code does not mention it at all. In order to be able to object to their personal data being processed for the purposes of NFI data-matching, data subjects must first be aware that this is one of the likely uses of their data. This generously assumes that every single voluntary NFI participant disclosed its participation in the NFI data-matching exercise to the individuals whose data it processes. But there is no way of testing this assumption. As stated in the paragraphs above, the full list of voluntary NFI participants is not public. This makes it impossible for individuals and civil society to verify whether all participating authorities disclose – as they should – their participation in the NFI data-sharing exercise in their privacy policies.

As it currently stands, the Code of Practice does not include sufficient safeguards to guarantee the exercise of data subjects' right to object.

Further concerns under Article 8

The Cabinet Office has separate and additional obligations imposed by Article 8 of the European Convention on Human Rights (ECHR), which protects the right to a private life.

European Court of Human Rights (ECtHR) jurisprudence makes it clear that Article 8 is engaged where personal data is collected and stored by State authorities, and that domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of Article 8. In *S. and Marper v.the United Kingdom*, the ECtHR determined that the need for such safeguards was all the greater where the protection of personal data undergoes automatic processing, as is the case in the NFI data-matching exercise.

There can be little doubt that the NFI, and in particular its proposed expansion, interfere with Article 8. However, as the right to privacy is not absolute, the ECtHR accepts that an interference may be justified if it is in accordance with the law, pursues a legitimate aim, and is necessary in a democratic society. An interference will be considered necessary if it answers a "pressing social need", if it is proportionate to the legitimate aim pursued, and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". As flagged elsewhere,[33]

[33] Amberhawk, *The return of the database state: mandatory data matching and expansive data sharing*, 18 February 2021. Available at:

it is unclear whether all of the proposed expansions of the NFI are necessary in a democratic society. There is no evidence that the government has balanced the potential benefits of the changes to the NFI against private life interests. This assessment is crucial to ensure that the proposed expansion of the NFI is compatible with Article 8.

As a matter of priority, the government must undertake an assessment of the proposed expansion of the NFI and its compatibility with human rights law beyond data protection, and make that assessment public.

Recommendations

PI calls on the Cabinet Office to do the following, at the earliest possible opportunity:

- Disclose any assessments and evaluations analysing, or purporting to analyse, the effectiveness of the NFI for the existing fraud detection purpose, and each of the proposed additional purposes, including:
  - The parameters for measuring success, and the suggested future applications which are the subject of the Consultation (e.g., detecting at least 100 instances of fraud per year, or 100 crimes per year);
  - The total number of searches carried out so far as part of the NFI data-matching exercise, disaggregated by each participating entity;
  - The number of "hits" so far (instances where the data-matching exercise flagged an inconsistency worth pursuing);
  - The number of times that a "hit" was accurate;
  - The number of times that a "hit" resulted in enforcement action; and
  - The number of times that enforcement action was successful.

- Disclose the full list of mandatory and voluntary participants to the NFI;
- Disclose all dataset specifications, both current and projected, across mandatory and voluntary participants to the NFI;
- Disclose any meaningful limits to the amount, categories and granularity of data accessed by voluntary participants, as compared to mandatory participants; alternatively, provide an explanation as to why the level of access is the same;
- Sufficiently describe, and distinguish, the rights and opportunities available to data subjects whose data is shared with the NFI by mandatory and voluntary participants;
- Amend the Draft Code to include data protection terminology reflecting the full implications of NFI data-matching, including profiling, and warn against the legal implications of automated decision-making;
- Clarify the roles and responsibilities owed to data subjects by participants to the NFI, and the Cabinet Office;

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

- Make changes to the Draft Code so that the data retention period applicable to the NFI is clear;
- Require all participating entities to share the following information with their data subjects:
    - Clarify that their data may be used for a data-matching exercise;
    - Describe all the potential entities with which their data may be shared as part of the data-matching exercise, and for which purposes those entities may access the data subject's data; and
    - For each of the NFI powers, provide examples of data matches and the possible interpretations and inferences that can be made from these data matches.

- Publicly commit to disclosing any future Data Protection Impact Assessments issued in relation to the NFI;
- Provide information as to how, if at all, the NFI will seek to mitigate disproportionate adverse impacts on groups sharing protected characteristics for each of the new purposes; and
- Disclose any assessments made to ensure that the proposed update to the NFI is compatible with Article 8 ECHR.