NEW ECONOMICS FOUNDATION

DIGITAL SELF-CONTROL

ALGORITHMS, ACCOUNTABILITY, AND OUR DIGITAL SELVES

NEW
ECONOMICS
FOUNDATION

CONTENTS

EXECUTIVE SUMMARY

Algorithms are not new, but thanks to the digital revolution, they're becoming part of almost every aspect of our lives. They're indispensable in the online world due to the need to sort the huge volumes of information online in order to make the Internet the valuable resource that it is today. As the digital economy has grown, the reach of algorithms has extended. Today they're responsible for almost 40% of stock trades in the UK. They fly planes for over 95% of the time the planes are in the air. And they may soon be driving our cars. Algorithms are also expanding into new areas to help people make decisions about whether to offer an applicant a job interview, whether offenders will reoffend, and what social care provision a service user needs. Despite presenting a technological veneer of objectivity around their decisions, algorithms, and the data collection that powers them, are designed by people and shaped by human decisions.

We're moving towards a society where access to both public and private services is mediated through algorithms. Algorithms are now entering increasingly controversial areas and making decisions with real implications for people's lives. These algorithms analyse vast amounts of data about us to generate a score which will decide whether we can access a good or service. In the public sector, under austerity, tightening budgets have led to a need to use decision-making algorithms to save on staff costs and help decide how to allocate funds and services.

There are currently thousands of digital profiles of each of us, collated from data trails we've left online. Acxiom, one of the largest data brokers on the planet, concedes that about 30% of the data held in each profile is incorrect. Given the poor quality of the profiles being built about us and the increasing use of digital profiles in the public and private sectors, incorrect decision-making could have series ramifications in our lives.

This report finds that as algorithms enter increasingly sensitive areas of our lives, we need to have meaningful accountability for those who create and deploy algorithmic decision systems, especially in areas where decisions have a significant impact on individuals. We also must ensure that we, as individuals, are not held accountable for things we didn't do, or for being someone we are not.

RECOMMENDATIONS

1. Establish an accountable standard for algorithms governing access to goods, services, and law enforcement.

This standard would ensure that individuals **know when they are interacting with an algorithm.**

Algorithm developers should:

- Ensure **clear responsibility of algorithmic decision systems** with rules about who is formally and legally responsible for the system.
- Provide **details of the accuracy of the system** together with a description of their function and intention and a list of data inputs used in deploying the system.
- Provide a statement **highlighting any biases** and **confirming that they are not discriminatory**.
- Ensure they have **a secure and verifiable audit trail**.
- Extend **right to an explanation** to any decision involving an algorithm.

2. Create a Digital Passport system and an independently run National Data Store

To ensure that digital profiles are accurate, and that individuals are not being scored incorrectly, we recommend the development of a new alternative that ensures we have ownership of our digital profile while prioritising our privacy.

Government should create a Digital Passport system. This would be an independently governed piece of **decentralised infrastructure that allows us to prove our digital identity online**. In addition, they should create an independently run National Data Store. This would be a decentralised digital data store for our profiles that individuals can **access and control through an easy-to-use app or website**. While the state would initiate the system, its structure and architecture would ensure that they don't have easy access to it and their role is restricted to establishing and enforcing the rules and rights needed for the system to work.

We would have direct control over the data, verified attributes, and inferences in our profiles. The definition of personal data would also be extended to include inferences produced in other profiles, too. We would be able to differentiate the data that we want to share with different types of systems and algorithms. The independent organisation running the National Data Store would also stipulate conditions of access, so that companies, government agencies, and municipalities can tap into this identity system in lieu of privately maintained digital profiles and reputation scores.

For companies who chose to continue to use their own systems and profiles, algorithmic decisions that have been based on incorrect information or unverifiable and unreasonable inferences should result in fines for the company deploying the algorithmic decision system and damages for the person involved.

1. INTRODUCTION

Algorithms are now part of almost every aspect of our lives. They're responsible for almost 40% of stock trades in the UK.[1] They fly planes for over 95% of the time the planes are in the air.[2] And they may soon be driving our cars, too. In the Internet age, our every interaction the World Wide Web is mediated by algorithms. Algorithms decide what search results to show us, recommend potential friends, and facilitate what adverts we see. They will soon form part of the decision about whether we get a loan or what price we're quoted for an insurance policy. And they're expanding into new areas to help people make decisions about whether to offer an applicant a job interview,[3] whether offenders will reoffend,[4] or what social care provision a service user may need.[5]

We're moving towards a society where access to both public and private services is mediated through algorithms. These algorithms analyse data about us to generate a score which will decide whether we can access services.[6] As a society, our 'hopes of feeling in control of these systems are dashed by their hiddenness, their ubiquity, their opacity, and the lack of obvious means to challenge them when they produce unexpected, damaging, unfair or discriminatory results'.[7] To rectify this, we need meaningful accountability for those who create and deploy algorithmic decision systems, especially in areas where decisions have a significant impact on us, as well as ensure that we, as individuals, are not held accountable for things we didn't do, like default on a debt, or for being someone we are not.

Modern algorithms analyse huge volumes of data to identify correlations. We need to be wary of drawing conclusions which conflate correlation, even very strong correlation, with actual causation. For example, US spending on science, space, and technology correlates highly with the number of suicides by hanging, strangulation, and suffocation in the USA.[8] But while there is correlation, there is no suggestion of causation between these two datasets. Reducing US spending on science will not reduce the number of suicides. While these two datasets correlate highly, one is not a good predictor for the other since the two datasets could diverge at any time.

The mass implementation of algorithms creates many opportunities to create inaccurate or unfair results. These can take three forms:

- The algorithm could be badly designed so that despite accurate information being fed in the system, it produces incorrect results (e.g. it thinks that 1+1=3).

- The algorithm could use data points that are prohibited or protected by law – or infer protected information via proxies (e.g. using postcodes to infer race). Algorithmic systems have proven very capable at establishing proxies for prohibited characteristics that allow them to avoid using prohibited data points directly. In many cases, the algorithm's use of proxies is not an intentional effort by the algorithm's programmers, but is developed by accident as the system looks for meaningful correlations and patterns in the data. This can make uncovering their use more complicated.

- Finally, the algorithm could use data or inferences contained in a digital profile about a subject that are incorrect or unfairly inferred.

Accountability is missing from our current use of algorithmic decision-making. Just as we need to hold those who design and deploy algorithms accountable for their results, we also need to define how far algorithms should be able to hold us accountable for our actions and characteristics.

Today, in an economy where data plays an increasingly central role, private companies create digital profiles for us, based on what data they can gather. But these digital representations of us can lead to extra-digital consequences. If our digital profile shows that we have outstanding debt, then we will be held accountable for that, even if no debt exists in real life. There are literally thousands of digital profiles of each of us, which are used to make decisions about services we can access. Currently, any business can create digital profiles on anyone (provided they can justify the data gathering under the EU General Data Protection Regulation) with no duty to ensure that their data is accurate. At the same time, we don't have easily exercisable rights to query and correct what data is being held about us, especially since profiles are often sold multiple times to third parties. This must change if we are to ensure that we're not being held accountable for something we did not do or character traits that we do not exhibit.

This report explores the two sides of the accountability question to ensure that we don't lose agency and control over the algorithms deployed to score and categorise us. To do this, we must have the necessary information and power to hold those who deploy such systems to account, be they public or private. At the same time, we examine the world of digital profiles and sketch an alternative vision for our digital selves. The new system will protect us and our data while making proving our identity online easier and giving us real control over our digital selves.

2. MAKING ALGORITHMS ACCOUNTABLE

Algorithms, and the data that powers them, are designed and created by people. Even algorithms that evolve on their own are still shaped by human-made design decisions: rules about what to optimise, and choices about what training data to use. 'The algorithm did it' is not an acceptable excuse if algorithmic systems make mistakes or have undesired consequences.

Humans, corporations, and public bodies should always be accountable for the systems they deploy. For proper accountability, it is necessary but not sufficient to ensure there's clear responsibility within an organisation deploying an algorithmic decision-making system. Importantly, not all algorithms have the same power over our lives and therefore they shouldn't all carry the same compliance costs. An algorithm which assesses the strength of someone's proposed password should not be subject to the same regulation as one that helps decide whether to grant someone else parole. Further work is needed to refine what types of algorithms should be included in the regulatory framework, and in which situations.

For those systems that need to comply, accountability should imply a wider 'obligation to report and justify algorithmic decision-making, and to mitigate any negative social impacts or potential harms'.[9] Following the work of Nick Diakopolous, there are five core strands of accountability for algorithms that all need to be present in a well-designed system:

1. **Responsibility.** For any system, there should be a named person with the authority to deal with the effects of the deployment of the algorithm. It is important that those deploying these systems take responsibility for the outcomes they produce and that those affected can seek redress.

2. **Explainability.** Any decisions produced by an algorithmic system should be explainable to the people affected by those decisions.

3. **Accuracy.** No system is perfect. Even the best algorithms will make mistakes. Understanding this is therefore critical and should require those deploying these systems to understand sources of potential errors and statistical uncertainty.

4. **Auditability.** Algorithms should be developed and deployed so that third parties, both private and public, can interrogate their behaviour.

BOX 1 – ALGORITHMS IN THE PRIVATE SECTOR

Many large companies have been using algorithms to sift through job applications and help them select candidates.[10] Although in wide use, Amazon recently abandoned the practice because 'its new system was not rating candidates for software developer jobs and other technical posts in a gender-neutral way.'[11]

The financial tech (fintech) industry is exploring the use of social network data to provide financial services to those without an established credit history.[12] Lenddo, a fintech company, issued 10,000 loans based purely on social network data, and claimed that its model was just as good as traditional models and should improve over time. [13]

Airlines have been under pressure recently as evidence mounts that they use an algorithm to ensure that family members travelling together, including those with small children, are split up unless they agree to pay the additional charges for specific seat allocation.[14] This is despite the Royal Aeronautical Society confirming that "the separation of passengers traveling together could have negative consequences for safety on board."[15]

Proof that these systems really are entering every corner of modern life is Predictim, a company which uses algorithmic decision-making to vet prospective babysitters for potential drug use, bullying, or bad attitude.[16]

5. **Fairness.** All algorithms making decisions about individuals, groups, or communities should be evaluated for discriminatory effects. The results of the evaluation and the criteria used should be publicly released and explained.

Concern over the rapid proliferation of algorithms is really a concern over the sectors they're entering and the types of decisions they're making. If their role in the digital age had remained focused on helping sort the information of the Internet, by organising search results, or recommending similar products, then there would be less urgency for reform (although vigilance about their potential effects would still be important). Extra vigilance is required now that algorithms are entering much more controversial areas and making decisions with real implications on our lives.

Modern algorithms have evolved primarily within the private sector (Box 1). There is an increasing interest within the public sector for using algorithmic decision-making (Box 2). There is also concern from academics and commentators that major companies and governments, both local and national, are becoming overly reliant on algorithmic decision-making systems.[17] A recent report by the House of Commons Science and Technology Committee argues that the introduction of technology and algorithms have the potential to improve public services and drive innovation.[18] This, coupled with the tightening of government budgets under austerity, means there's a strong drive to seek opportunities to implement algorithms which can save on staff costs. Some in the public sector are seeking to genuinely improve public services, while others are more concerned with how increasingly stretched resources can be spread out to prioritise those most in need. Faced with the prospect of not being

BOX 2 – ALGORITHMS IN THE PUBLIC SECTOR

Norfolk police have been using an algorithm to help decide whether to investigate reported burglaries by analysing 29 factors. These factors are not public, partly to protect the intellectual property and partly to prevent would-be criminals from gaming the system.[19] At a time when the frequency of domestic burglaries has increased by 32%,[20] police numbers have been reduced by 15%.[21] Limited resources are forcing police forces to develop mechanisms to help them prioritise their work.

At least five local authorities have started using an algorithm to identify families with children at risk of abuse.[22] The algorithm draws on a wide range of data for the child and surrounding family members including school attendance and exclusion data, housing association repairs and arrears data, and police records on antisocial behaviour and domestic violence. Again, this is happening in an environment where council budgets have been severely reduced and local authorities are now targeting their available resources to those most in need, since they cannot meet all the demand for their services.

Brent Council is working with IBM to implement an algorithm to help it identify children at risk of gang exploitation.[23] The Council also views the algorithm as a potential revenue-generating product which it could sell to other councils.[24]

Algorithms are also entering the health system using x-rays and other scans to create diagnoses. They have already been shown to outperform radiologists.[25]

able to deliver essential services, the public sector is bringing in algorithms to help decide who most needs (or sometimes, 'deserves') access. Although this can be seen as bringing objectivity to hard decisions, in fact the systems often reflect and reinforce the existing biases and practices of those bureaucracies.[26] At the same time, they're also being increasingly used in the fight against complex social problems, such the identification of child abuse online or the prediction and prevention of crime. While algorithms can be helpful in this kind of decision-making, there are risks in relying on them too heavily and ceasing to emphasise human judgement. As well as highlighting that algorithms cannot solve complex social problems, the report notes:

Algorithms, in looking for and exploiting data patterns, can sometimes produce flawed or biased 'decisions'. As a result, the algorithmic decision may disproportionately discriminate against certain groups, and are as unacceptable as any existing 'human" discrimination'.[27]

This problem becomes more acute when companies or governments depend on private partners for algorithms whose development they have little or no control over. The expanding use of inscrutable privately developed algorithms in the public sector, in everything from child services to policing, undermines the ability of civil society to hold companies and public bodies to account, because these digital processes are 'black-boxed' and often qualify as trade secrets.[28] This leaves individuals affected by these systems with no way to understand or challenge the basis upon which decisions have been made, or assess the efficacy and fairness of the overall process.

2.1 RECOMMENDATIONS

As algorithms increasingly enter sensitive areas of our lives, we need to ensure that there is clear accountability for decisions made by algorithmic systems. These requirements should apply to all algorithms that are part of the system governing access to goods, services, and law enforcement with further research needed to determine whether algorithms in other areas should also be included. We have a right to know when we are interacting with an algorithm. Every algorithm should be independently verifiable to ensure they work correctly, and algorithm developers should provide an independently verified statement that they are free from bias and discrimination. There needs to be secure and verifiable audit trails and compensation for those unfairly harmed by an algorithm's decision.

To increase the overall transparency of algorithmic systems, we need to **introduce a new right to know we are interacting with an algorithm**. Systems should be required to make people aware when they have been the subject of an automated decision or a decision-assistance system with a real person ultimately making the final decision. No extra information about the algorithm would need to be provided at this stage but should there be a concern this new right will be first point of call when seeking to hold these systems accountable by linking to details about to how to get additional information or raise concerns. This could be enacted through an amendment to the existing General Data Protection Regulation (GDPR) or new primary legislation.

In addition, creators of algorithmic decision-making systems being used in the UK or on UK residents should produce and make publicly available the following documentation:

1. **Clear responsibility of algorithmic decision systems** with rules about who is formally and legally responsible for the system. The default would be that the company using the system is responsible for its results, but companies could contractually delegate responsibility to the system's creator. They would also be required to list a named person responsible within the company to address any correspondence.

2. **Details on the accuracy of the system**, together with a description of its function, intention, and a list of data inputs used in its deployment.

3. Creators should provide a **statement confirming that the algorithm does not use any protected characteristics** while making its decisions. This will be legally binding so that, should any claims of discrimination arise from the algorithm's design (rather than its implementation or the use of incorrect profile data) the creator would be legally responsible. Creators should also use third parties to confirm the accuracy of the algorithm and provide indemnity against future claims

4. Systems, especially those in the public sector, should be created so that a **secure and verifiable audit trail** can be used to monitor the activity of the algorithm and which data it queries in order to help with investigations into its decisions.

The GDPR's **right to an explanation for individuals**[29] **should be extended to any decision involving an algorithm** within the scope previously mentioned. Currently, this right only applies to decisions made solely through automation, with no human involvement whatsoever. The wording in the GDPR does not make it clear when this right can be triggered. In addition, even the explanation mandated by the GDPR as 'meaningful information about the logic of processing'[30] is not in line with current machine learning technologies which are constantly adapting and updating their processing logic.[31]

3. RECLAIMING OUR DIGITAL SELVES

There are currently thousands of digital profiles of each of us, collated from data trails online. Some contain rich histories, others just single data points. Acxiom, one of the largest data brokers on the planet, concedes that about 30% of the data held in each profile is incorrect.[32] Given the poor quality of the profiles being built of us and the increasing use of digital profiles in the public and private sectors, this poses a significant risk that we'll be held accountable for things we didn't do or for being a person that we are not, with major implications for our lives.

It's important to note that not all requests to confirm identity or attributes should be treated the same. In some use cases, it is critical to correctly establish our identity or provide an accurate profile that a system can query in order to ascertain whether access to the good or service should be provided. Today, in the real world, we have many identities online. When asked for a name to log in to a public Wi-Fi network, it is understandable that some of us lie to minimise pervasive tracking. The recommendations set out in this report as well as our previous report, 'Blocking the data stalkers'[33] would create such a different data economy that we would be less concerned about providing accurate data, since the onward sale of data would be restricted, the AdTech industry depersonalised, and algorithms made accountable. Reliable digital profiles would mean that individual companies and data brokers would be less able to gather and exploit the data that we share. In addition, our proposal allows key attributes to be validated, like age or location, without revealing additional personal data.

In the UK, the most interesting example of digital profiles is within the credit score system, which feeds the data it collects into algorithms to determine our ability to repay a loan. In this system, a small number of companies maintain profiles about us, mainly focused on our financial transactions, loans, and bill payments. We have the right to access this information and can challenge and have them remove incorrect data held. Based on these factual data points, companies draw some inferences (like how likely we are to change jobs). They then use all the data to generate a credit score which is shared with third parties querying our potential to take on debt. The credit report system gives us the right to correct incorrect information – but importantly it does not give us any right to query the inference (credit score) made about us.

The prospect of other decision-makers mimicking the governance of the credit score system is problematic for two reasons. First, although it is conceivable that we would check and correct three credit score profiles (57% of people have checked their profile at least once in the last year),[34] most of us are unable to check the many thousands of digital profiles out there, many of which are managed by companies that we have never heard of.

Second, for the right to check and correct profiles to be meaningful, we must have some control over the inferences these companies are making about us.

Our digital profiles are full, not just of objective and contestable facts (age, place of birth, address, etc.) but also of inferred characteristics. In fact, many of the most 'useful' and monetisable aspects of our profiles are inferred

BOX 3 – DIGITAL PROFILES ARE ALREADY RUINING LIVES[35]

Catherine Taylor's world was turned upside down when a data broker, ChoicePoint, incorrectly linked her to a criminal charge of intention to supply methamphetamines.[36] The data broker then sold her file on many times so that the original error was replicated widely across the many digital profiles maintained about her.

Luckily for Catherine, she was able to find this incorrect data and communicated with ChoicePoint so that they could remove the record. However, this did not rectify the error in all the systems that had bought the incorrect data. Catherine was forced to personally contact all the other brokers and even file lawsuits to get the offending data removed.

The error costed her job interviews, as employers were scared away by the black mark against her name. It took over four years for her to find a job. In the meantime, she was rejected for an apartment she wanted to buy and couldn't even get credit for a new washing machine.

Although Catherine was able to remove almost all the incorrect data, it took a huge toll on her personally, consuming lots of time and effort while exacerbating health problems. But at least Catherine was aware of the offending data. Many people could be affected by this problem without knowing the reason or having the time and patience to resolve the issue.

data, including data that has been inferred from other inferred data points. Examples could be our interest in a certain topic or product; whether we're getting married or having a child in the near future; or our mental health and imminent suicide risk or attempts. These inferences are currently made mainly to target advertising, but also to personalise what we see on each website. Inferences are never certain – although some can be verified or proven at a later date if additional information is forthcoming. They merely generate predictions with a set correlation percentage. The extensive use of inferred data to make sensitive decisions about us 'poses substantial and novel risks not only to identity, but reputation and the choices offered to an individual by data-driven services'[37] because incorrectly inferred data can literally ruin lives (Box 3).

A critical question which will inform how we try to tackle this emerging problem is whether inferences about us constitute 'personal information' as defined and protected by the GDPR.[38] They seem to be excluded under the current interpretation, but the Article 29 Working Party,[39] established by the EU Commission, argues that data 'likely to have an impact on a certain person's rights and interest' should constitute personal data.[40] Inferences must be categorised as personal data, if we are to mitigate the risks of incorrect algorithmic decisions.

We also need to distinguish between two types of inferred data – verifiable and non-verifiable – as this will have a major impact on potential rectification.[41] Some inferences can be verified against an observable fact. For example, income range can be validated by producing a payslip. Other inferences are subjective (e.g. Simon is a high-risk driver) or predictive (e.g. Simon will do something in the future) and therefore cannot be verified easily and objectively.

The area of digital profiles is ripe for reform. We desperately need a system that will allow us to securely identify ourselves online without leaking unwanted data. A current option that many websites use is to ask users to log in using a Google or Facebook account. This not only provides considerable information to the website but also allows Google or Facebook to further expand their user profiles. This will become particularly important when new legislation comes into force in April 2019 requiring adult content sites to verify that users are over 18.[42] Currently, the most common way to verify this information is through bankcard details. Adult sites will be able to collect a huge database of people's identification, banking information, and site preferences. This poses huge risks, from simple theft of banking details to more sophisticated blackmail of individuals.

BOX 4 – ESTONIA

One current example, to learn from rather than mimic, is Estonia. Estonia has been on a journey since 1997 when it put 99% of government services online. In 2014, it launched e-residency which allows people to verify their ID online through a cryptographic key. It was used initially just for government services but is now also usable within the private sector. A recent report by Kattel & Mergel identifies some of the critical success factors to learn from. These focus especially on governance, which harnessed the insights of the public and private sectors looking at the system holistically; design, with a central focus on decentralisation and interoperability, meaning that different systems should be able to talk to each other; and security.[43]

Mastercard and Microsoft recently announced a partnership to look at creating 'a universally-recognized digital identity'[44] system. Their press release says that a new identity system should put 'people in control of their digital identity and data' and be 'a system that puts people first, giving them control of their identity data and where it is used'.[45] In reality, however, this would mean all people would have to centralise all of their data within this new private venture, creating massive potential for surveillance.

We are at a crossroads. The profile system of the future can either be built by the private sector to monetise our data, or by a new alternative that ensures we have real ownership and agency over our identity and profile while prioritising our privacy.

3.1 RECOMMENDATION

We believe that government should initiate the creation of an independently governed piece of decentralised infrastructure so that we can prove our digital identity online (Box 4). We call this the **Digital Passport**.[46] In addition, they should initiate the creation of a decentralised independently run digital data store for our profiles that we can access and control through an easy-to-use app or website. We call this the **National Data Store**.

Although we should rightly be cautious of placing too much data and power in the hands of the state, as Evgeny Morozov explains: 'For all the fears of government surveillance, we are still better off under a state-enforced system of digital rights than under complete submission to the whims of today's tech barons.'[47] In addition, while the state would initiate the system, its structure and architecture would ensure that they don't have easy access to it and their role is mainly in establishing the rules and rights needed for the system to work.

This new secure and decentralised Digital Passport and the National Data Store would be managed by an independent body. Initially it would have the data that we submit to the state in order to verify our identity (age, place of birth, date of birth, etc.). But through extending the right to data portability in Article 20 of the GDPR[48] to include inferred data, it would be very simple for people to incorporate data from other sources online or add data directly to our profile. The government would then commit to proactively providing us with our own data held by multiple different government departments. Special consideration would need to be given to whether the most sensitive data such as health or home office data should be transferred automatically. We would have the option of either sticking with the minimum profile or working to make it as complete as possible by integrating other sources of data, such as social media or financial data, which could make it easier to get a loan or insurance.

We would have direct control over the data, verified attributes, and inferences in our profile. The definition of personal data should also be extended to inferences produced in other profiles, too. We would be able to differentiate the data that we want to share with different types of systems and algorithms – for instance forbidding social media data to be shared with financial institutions. Just as in the physical world, we should be able to show different aspects of ourselves under different circumstances, just as we do when we turn up for a job interview in a suit rather than party clothes.

Through a deliberative process with a cross section of the population, standards would need to be developed which ensure that we are protected by default. These standards would also define when it is acceptable for the new independent organisation governing the National Data Store to form inferences about us, including looking into whether there may be specific use cases when high-risk inferences like sexual orientation and mental health status might be appropriate. At the same time, thresholds need to be agreed to ensure the correct level of reliability of the inferences. Following these guidelines and principles, the organisation would then also process the data that we have submitted and produce inferred data about us to populate our profiles. We would retain control over which companies and their algorithms had access to which fields in our profiles.

The organisation would also stipulate conditions of access, so that companies, government agencies, and municipalities can tap into this identity system in lieu of privately maintained digital profiles and reputation scores through a simple API, which is the code that allows two pieces of software to interact with each other. This would be able to provide not only a Digital Identity token, a cryptographic token which could validate a user's verified attributes (such as whether they are over 18) but could also be used to provide key inputs to algorithms online. Algorithms would then no longer have to rely on their own or third party profiles for data, thereby reducing the overall demand for widespread data collection.

Another independent organisation, modelled on the Audit Commission, would manage the audit of the algorithms and ensure that the body that contained our profiles was privacy-aware, with protection of our data at its heart and focused on enabling decentralised solutions.

In addition, we need to ensure that companies who chose to continue to use their own systems and profiles are held accountable for their actions. Therefore algorithmic decisions that have been based on factual or verifiable profile information that is incorrect or based on an unverifiable and unreasonable inferences[49] that cause harm to the person could be challenged with fines for the company deploying the algorithmic decision system and damages for the person involved.

With the right blend of fines and obligations and coupled with the poor data quality of existing digital profiles generally, there would be few companies who would continue to build and use their own profiles. Most would jump at the chance to use data that was guaranteed to be accurate, where its use generated no potential liabilities for the business, and worked with the cooperation and consent of the people.

BOX 5: RECOMMENDATIONS

1. Establish an accountable algorithm standard for algorithms governing access to goods, services, and law enforcement

This standard would ensure that individuals should have **a right to know when they are interacting with an algorithm.**

Algorithms should:

- Ensure **clear responsibility of algorithmic decision systems** with rules about who is formally and legally responsible for the system.
- Provide **details on the accuracy of the system** together with a description of their function, intention and a list of data inputs used in deploying the system.
- Provide a statement **highlighting any biases** and **confirming that they are not discriminatory**.
- Ensure **a secure and verifiable audit trail** of the algorithm.
- The **right to an explanation should be extended** to any decision involving an algorithm.

2. Create a Digital Passport system and independently-run National Data Store

In order to ensure that our digital profiles are accurate, and that we're not being scored incorrectly, we recommend the development of a new alternative that ensures we have ownership over our digital profile while prioritising our privacy.

Government should create a Digital Passport system. This is an independently governed piece of **decentralised infrastructure so that we can prove our digital identity online**. In addition they should create an independently-run National Data Store. This is a decentralised digital data store for people's profiles that they would **access and control through an easy-to-use app or website**. While the state will initiate the system, its structure and architecture will ensure that government does not have easy access to it and their role will be restricted to establishing and enforcing the rules and rights needed for the system to work.

We would have direct control over the data, verified attributes and inferences in our profile and would also extend the definition of personal data to inferences produced in other profiles too. People would be able to differentiate the data that they wanted to share with different types of systems and algorithms. The organisation would also stipulate conditions of access, so that companies, government agencies and municipalities can tap into this identity system in lieu of privately maintained digital profiles and reputation scores.

For companies who chose to continue to use their own systems and profiles, algorithmic decisions that have been based on incorrect information or unverifiable and unreasonable inferences should result in fines for the company deploying the algorithmic decision system and damages for the person involved.

4. CONCLUSION

We have choices about the digital future that we want. If we continue to cede agency and control, our data will be held by largely unaccountable corporations who maintain huge profiles of us, containing lots of incorrect information.

If we implement these recommendations, however, we would have a digital identity and profile that we control, where society has proactively set the limits of what is acceptable, and where we actively monitor the systems that maintain our data and generate useful inferences. We would also have a robust system of accountability for those deploying algorithmic systems where we would always know if we were interacting with an algorithm and would be able to seek additional information as well as further redress should the decision cause us material harm.

ENDNOTES

[1] Speech by Mr Andrew Haldane, Executive Director, Financial Stability, Bank of England, at the Oxford China Business Forum, Beijing, 9 September 2010. Retrieved from https://www.bis.org/review/r100909e.pdf

[2] Templeton, P. (2016). How much do Airline Pilots actually fly and airliner by hand? Retrieved from https://pilotjobs.atpflightschool.com/2016/07/27/how-much-do-airline-pilots-actually-fly-an-airliner-by-hand/

[3] Koenig, K. (2018).Your next recruiter could be an algorithm. Retrieved from https://money.usnews.com/careers/applying-for-a-job/articles/2018-08-22/your-next-recruiter-could-be-an-algorithm

[4] Tashea, J. (2018). Courts are using AI to sentence criminals.That must stop. Retrieved from https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/

[5] Guardian Editorial. (2018, September 17). The Guardian view on AI in social work: algorithms don't have all the answers. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2018/sep/17/the-guardian-view-on-ai-in-social-work-algorithms-dont-have-all-the-answers

[6] McCann, D. & Hall, M. (2018). What's your score? Retrieved from https://neweconomics.org/2018/07/whats-your-score

[7] Edwards, L. & Veale, M. (2017). Slave to the Algorithm? Why a‘right to an explanation’is probably not the remedy you are looking for. *16 Duke Law and Technology Review, 18.*

[8] http://www.tylervigen.com/spurious-correlations

[9] Fairness Accountability and Transparency in Machine Learning. (2018). Principles for Accountable Algorithms. Retrieved from http://www.fatml.org/resources/principles-for-accountable-algorithms

[10] Danieli, O., Hills, A. & Luca, M. (2016). How to hire with algorithms. Retrieved from https://hbr.org/2016/10/how-to-hire-with-algorithms

[11] Higginbottom, K. (2018).The Pros and Cons of algorithms in recruitment. Retrieved from https://www.forbes.com/sites/karenhigginbottom/2018/10/19/the-pros-and-cons-of-algorithms-in-recruitment/#

[12] Vasager, J. (2016). Kreditech: a credit check by social media. Retrieved from https://www.ft.com/content/12dc4cda-ae59-11e5-b955-1a1d298b6250

[13] Hynes, C. (2017). How social media could help the unbanked land a loan. Retrieved from https://www.forbes.com/sites/chynes/2017/04/25/how-data-will-help-drive-universal-financial-access/#1cf01b7657e6

[14] Doctorow, C. (2018). UK minister says airline used‘exploitative algorithms’to split up families unless they paid extra. Retrieved from https://bbs.boingboing.net/t/uk-minister-says-airlines-used-exploitative-algorithms-to-split-up-families-unless-they-paid-extra/133636

[15] Green Claim. (2018). Airlines might be using an algorithm to separate you from your fellow travellers. Retrieved from https://www.greenclaim.com/news/2018/11/29/airlines-might-be-using-an-algorithm-to-separate-you-from-your-fellow-travellers

[16] Harwell, D. (2018). Wanted:‘the perfect babysitter.’Must pass AI scan for respect and attitude. Retrieved from https://www.washingtonpost.com/technology/2018/11/16/wanted-perfect-babysitter-must-pass-ai-scan-respect-attitude/?noredirect=on&utm_term=.f9dd37884d50

[17] Rainee, L. & Andersen, J. (2017). Code-dependent: Pros and cons of the Algorithm age. Retrieved from http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/

18 UK Parliament. (2018). Algorithms in Decision Making. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/351/35102.htm

19 Charette, R. (2018). Norfolk Constabulary using controversial algorithm to help decide if burglary investigation warranted. Retrieved from https://spectrum.ieee.org/riskfactor/computing/software/norfolk-constabulary-using-controversial-algorithm-to-help-decide-if-burglary-investigation-warranted

20 Travis, A. (2018). Rise in recorded crime is accelerating in England and Wales. Retrieved from https://www.theguardian.com/uk-news/2018/jan/25/knife-and-gun-rises-sharply-in-england-and-wales

21 Dearden, L. (2018). Police officer numbers hit record low as reported crime rises by 14% in England and Wales. Retrieved from https://www.independent.co.uk/news/uk/crime/crime-rises-statistics-england-wales-police-officer-numbers-record-low-government-tories-labour-cuts-a8178631.html

22 McIntyre, N. & Pegg, D. (2018, September 16). Councils use 377,000 people's data in effort to predict child abuse. *The Guardian*. Retrieved from https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse

23 McIntyre, N. & Pegg, D. (2018, September 17). Data on thousands of children used to predict risk of gang exploitation. *The Guardian*. Retrieved from https://www.theguardian.com/society/2018/sep/17/data-on-thousands-of-children-used-to-predict-risk-of-gang-exploitation

24 Brent Council. (2017). Safer Brent Partnership. Retrieved from https://www.brent.gov.uk/media/16407560/3-may-2017-safer-brent-partnership-annual-report-2016-2017.pdf

25 Armitage, H. (2018). AI rival radiologist-level X-ray screening for certain lung diseases. Retrieved from https://engineering.stanford.edu/magazine/article/new-algorithm-outperforms-radiologists-disease-diagnosis

26 Cave, S. (2019). To save us from a Kafkaesque future, we must democratise AI. Retrieved from https://www.theguardian.com/commentisfree/2019/jan/04/future-democratise-ai-artificial-intelligence-power

27 UK Parliament. (2018). Algorithms in Decision Making. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/351/35102.htm

28 Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press.

29 Information Commissioners Office. (2018). Rights related to automated decision making including profiling,. Retrieved from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

30 Edwards, L.& Veale, M. (2017). Slave to the algorithm? Why a'right to an explanation' is probably not the remedy you are looking for. *16 Duke Law & Technology Review, 18*.

31 Ruiz, J. (2018) Machine learning and the Right to an Explanation. Retrieved from https://www.openrightsgroup.org/blog/2018/machine-learning-and-the-right-to-explanation-in-gdpr

32 Hicken, M. (2013). Find out what Big Data knows about you (it may be very wrong). Retrieved from https://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/

33 McCann, D. & Hall, M. (2018). Blocking the Data Stalkers. London: NEF. Retrieved from https://neweconomics.org/2018/12/blocking-the-data-stalkers

34 Lamagna, M. (2018). More people are now checking their credit scores – heres why that pays. Retrieved from https://www.marketwatch.com/story/more-people-are-now-checking-their-credit-scoresheres-why-that-pays-2018-06-19

35 McCann, D. & Hall, M. (2018). Blocking the Data Stalkers. London: NEF. Retrieved from https://neweconomics.org/2018/12/blocking-the-data-stalkers

36 Pasquale, F. (2018). Our lives in a scored society. Retrieved from https://mondediplo.com/2018/05/05data

37 Wachter, S. & Mittelstadt, B. (2018). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*, Forthcoming . Available at SSRN: https://ssrn.com/abstract=3248829 3

38 Madge, R. (2017). Five loopholes in GDPR. Retrieved from https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b

39 The Article 29 Working Party was an advisory body made up of a representative from the data protection authority of each EU member state, the European Data Protection Supervisor and the European Commission.

40 Article 29 Data Protection Working Party. (2018). Guidelines on Automated Individual Decision Making and Profiling for the Purposes of Regulation 2016/679. Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

41 Wachter, S. & Mittelstadt, B. (2018). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*, Forthcoming . Available at SSRN: https://ssrn.com/abstract=3248829

42 Matthews-King A. (2018). Porn site age verification to in force by spring next year after delays, minister says. The Independent. Retrieved from https://www.independent.co.uk/news/uk/home-news/porn-site-age-verification-uk-pornhub-sex-online-adult-video-government-id-a8631886.html

43 Kattel, R. & Mergel, I. (2018). Estonia's digital transformation: Mission mystique and the hiding hand. UCL Institute for Innovation and Public Purpose Working Paper Series (IIPP WP 2018-19).

44 MastercardNews. (2018, December 3). 'Voting, driving, applying for a job, renting a home, getting married and boarding a plane: what do these all have in common? You need to prove your identity. In partnership with @Microsoft, we are working to create universally-recognized digital identity'. Retrieved from https://twitter.com/MastercardNews/status/1069601787852873728?s=03

45 Mastercard Press Release. (2018). Mastercard, Microsoft join forces to advance digital identity innovations. Retrieved from https://newsroom.mastercard.com/press-releases/mastercard-microsoft-join-forces-to-advance-digital-identity-innovations/#__prclt=IarCgTyK

46 'Digital passports' are gaining increasing attention from political parties as the scope of online digital identity becomes clearer. See the Labour Digital Democracy Manifesto for one example: Barbrook, R. (2016). The Digital Democracy Manifesto. Retrieved from https://d3n8a8pro7vhmx.cloudfront.net/corbynstays/pages/329/attachments/original/1472552058/Digital_Democracy.pdf

47 Morozov, E. (2018). The case for publicly enforced online rights. Retrieved from https://www.ft.com/content/5e62186c-c1a5-11e8-84cd-9e601db069b8

48 Art. 20 currently does not cover inferred or derived data and so at present the right would not extend to these kinds of data created about us by a third party

49 Based on the criteria that would be the outcome of the above process

NEW ECONOMICS FOUNDATION

WWW.NEWECONOMICS.ORG
info@neweconomics.org
+44 (0)20 7820 6300 @NEF
Registered charity number 1055254

NEF is a charitable thinktank, wholly independent of political parties and committed to being transparent about how it is funded.

WRITTEN BY:
Duncan McCann and Miranda Hall

COVER IMAGE:
www.istockphoto.com /Wenjie Dong

PUBLISHED:
February 2019

ACKNOWLEDGEMENTS:
Thanks to the Joseph Rowntree Charitable Trust for funding NEF's work on the digital economy.