

**Scrapping Subject Access Requests rights** – The Government is proposing to make it harder for you to make subject access requests. Vulnerable people will find it harder to hold the powerful to account.

*A company has been treating you poorly. You have complained about them a couple of times in the past. You put in a subject access request to try and get to the bottom of the problem. Due to previous complaints, they decide to mark you down as a 'vexatious complainant' and refuse your request to access the data they hold about you.*

**The Government wants to reduce the right we have to challenge unfair and biased decisions made by artificial intelligence.** From being assigned the wrong A-Level result to being unfairly rejected for credit. If the computer says no, you will have no right to appeal.

## 4 The politicisation of the Information Commissioners

**The Issue is:** Ministerial Power Grab – The Bill grants Ministers the power to set the priorities of the ICO. They will also gain control over the Information Commissioner's salary, and gain the power to veto the adoption of statutory codes and guidance. This will expose the ICO to political direction, pursuing cultural wars, corporate capture, and corruption.

*The government decides it needs to crack down on Trade Union's use of members' data for 'political purposes. It sets this as a priority for the ICO.*

**Discretionary Power to Ignore Complaints** – The ICO will be given discretionary power to ignore complaints. This will worsen their (already poor) track record, and allow the ICO to keep ignoring widespread and systemic abuses of data rights. Abuses that will only expand under these proposals.

*You make a complaint to the ICO. This is your last chance to try and get justice. You send the complaint off, only to receive an automatic email stating due to a backlog in cases your complaint has been triaged as not meriting further investigation'. You are told to go back to the organisation you are complaining about to resolve the situation.*

Watchdogs will be able to oversee your data

# STOP

# THE DATA DISCRIMINATION BILL



**ORG**  
OPEN RIGHTS  
GROUP

The Government's Data Discrimination Bill will gut critical and basic privacy laws in the UK and rip up GDPR protections. It spells the end of countless protections that prevent data discrimination.

**From workers and children to NHS patients and migrants, UK GDPR protects us all. But if the Government has their way, our basic rights to challenge abuse in the digital age will disappear.**

Without GDPR, students couldn't stop unfair algorithms from grading their A-level and workers couldn't challenge robo-dismissals. Victims of sexual violence would be subject to digital strip searches by Police and job applicants would face racist automated recruitment tools.

## 1 Digital Surveillance State

**The Issue is:** *The government wants to grant itself new powers to collect and share your data -*

The data discrimination bill will grant Government powers to rewrite the law, and compel organizations to share personal data they hold about you with the State and law enforcement authorities.

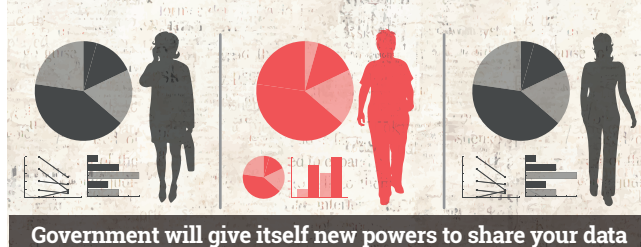
*HMRC decides it wants to automatically scan all personal financial transaction records to detect fraud under the National Fraud Initiative. The minister amends data protection rules to allow unfettered data sharing for "fraud detection". From banks, stores, and e-commerce retailers, every transaction you make is now sent automatically from your bank to HMRC where it is run through an AI algorithm to detect patterns of 'suspicious behaviour'.*

**BACK OUR  
CAMPAIGN TO  
STOP DATA  
DISCRIMINATION**

**ORG**  
OPEN RIGHTS  
GROUP



[www.openrightsgroup.org](http://www.openrightsgroup.org)



## 2 A Data Oligarchs Charter

**The Issue is:** Data transfers to other countries – The Government wants to transfer your data to other countries with lower privacy standards. This will create a 'Data Oligarchs' charter where data is laundered globally.

**Risking our EU adequacy status** – Huge volumes of trade rely on us having EU adequacy status. This status means the EU determines the UK to be a safer place for its citizen's data to be processed. In the race to the bottom of global standards, we risk losing this status.

**The imagery is:** A Data Oligarch is a powerful person or corporation that exploits information about you for personal gain. They use the information collected to exert power over other people. They operate in the shadows – taking advantage of low data protection standards in the same manner that off-shore tax loopholes are exploited.

## 3 Risks to workers, consumers and businesses

**The Issue Is:** Scrapping requirements for organizations to undertake digital privacy impact assessments this will increase the likelihood of organisations making costly errors.

Your company implements new systems and experiences a large data leak. This results in damages being paid and reputation damage. The lack of a proper digital privacy impact assessment was a contributing factor to the data leak occurring.

**Scrapping requirement for independent data protection officers** – Removing the requirement for an independent DPO will reduce the need to appoint an expert with sufficient autonomy and resources to ensure that people's data are protected. Instead, it will encroach on a "yes-man" culture, where privacy officers follow orders and do not promote positive change.

*You are sacked from your job as a data protection officer. A senior manager is placed in charge of data protection. However, they have no real expertise or interest in it and are being driven by other corporate agendas.*

**Your data may be laundered due to low privacy standards set by UK Government**

