

OPEN RIGHTS REPORT AND ACCOUNTS

YEAR ENDED 31 OCTOBER 2023



ABOUT ORG

Open Rights Group (ORG) is a UK based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 40,000 supporters, we are a grassroots organisation with local groups across the UK.

Our work on data protection and privacy includes challenging the immigration exemption to UK data protection law, defending the General Data Protection Regulation (GDPR) from attempts to water down its provisions, and challenging uncontrolled and unlawful data sharing by online advertisers.

openrightsgroup.org

Published under a Creative Commons
Attribution-ShareAlike 3.0 Unported Licence
<https://creativecommons.org/licenses/by-sa/3.0/>
except where stated.



ANNUAL REPORT OF THE DIRECTORS	1
OUR OBJECTIVES, MISSION, AND ACTIVITIES	2
INTRODUCTION	3
COMBATING BIG TECH AND PLATFORM POWER	5
CHALLENGING STATE INTRUSION INTO RIGHTS ONLINE	8
DIGITAL THREATS AGAINST COMMUNITIES MADE VULNERABLE BY SOCIETY	10
GRASSROOTS COMMUNITY, MEMBERSHIP AND ACTIVISM	13
INCOME AND EXPENDITURE ACCOUNT	14
BALANCE SHEET	15
NOTES TO FINANCIAL STATEMENTS	16



REPORT OF THE BOARD OF DIRECTORS

The Directors of the company present their annual report for the year ending 31 October 2023.

The Directors would like to thank our members, supporters, donors and grantors, who made our important work possible. The Directors would also like to thank our staff, volunteers, members of our local groups and Advisory Council for their hard work, support, tremendous knowledge and world-class expertise.

OUR OBJECTIVES, MISSION, AND ACTIVITIES

Open Rights Group is a UK-focused data and digital rights campaigning organisation. Founded in 2005, we have over 43,000 members and supporters and 13 local groups across the UK. For nearly two decades, ORG has been at the heart of the digital rights movement in the UK and an ally of activists and organisations across Europe.

Our vision

We envision a world where neither states nor corporations use digital technology to restrict or remove our rights. Our aim is to create a fair digital environment where technology supports justice, rights and freedoms to prevail over the narrow interests of the powerful.

Our mission

Our mission is to ensure that politicians, civil society and the general public are well informed and equipped to ensure that technology is directed to promote and protect human rights and social justice.

We advocate for human rights, such as free expression and privacy, and condemn and work against repressive laws or systems that deny people these rights.

Our unique perspective lies in the combination of technologists, policy experts, litigators, communication and campaign specialists both within our staff and across our network.

How we work

We campaign, lobby, go to court – whatever it takes to build and support a movement of individuals and organisations committed to freedom in the digital age.

- We **DEFINE** emerging harms and abuses through our research and forensic investigations.
- We **EQUIP** civil society partners to address data and technology issues in their work through our network support and coordination.
- We **MOBILISE** our members and supporters across the UK through our grassroots and public campaigns.
- We **PERSUADE** allies and adversaries through our policy advocacy.
- We **CONFRONT** threats to our fundamental rights through our strategic litigation

Our values:

- We believe in human rights;
- Our work is based on evidence;
- We are accountable to our supporters and operate with integrity;
- We believe in the importance of empowered people defending digital rights.



INTRODUCTION

2022 and 2023 witnessed ongoing challenges to digital rights. There was continued political uncertainty following Boris Johnson's resignation in July 2022. His successor, Liz Truss, was the shortest-serving Prime Minister in UK history, replaced after a just a few weeks by Rishi Sunak. Changes in leadership were matched by cabinet reshuffles, meaning changes to the ministers overseeing draft legislation that had huge implications for freedom of expression and privacy.

2023 was also the tenth anniversary of the Snowden revelations. Throughout the year, there were attacks on encryption in the UK, other Five Eyes countries, and Europe. Many of these attacks focused on Meta's rollout of end-to-end encryption in Messenger. ORG worked with tech companies and civil society around the world to challenge these attacks, particularly through our campaigning on the Online Safety Bill. It would be safe to say that, despite the improvements in oversight of security agencies, the essential agenda of access to everything, all the time, everywhere remains within the secret state.

Data protection reform through the Data Protection and Digital Information Bill continued despite widespread opposition from trade unions, civil society and charities. The Bill weakens the data protection rights of people in the UK but also threatens

the rights of European citizens – leading to concerns about its threat to the UK's adequacy agreement with the EU.

The flawed Shawcross review failed to address many problems with the government's Prevent programme, which is chilling freedom of expression and disproportionately impacting Muslims in the UK. ORG continued to push back on the securitisation of spaces for Muslims.

Generative AI models dominated the headlines in 2023, following the launch of ChatGPT in November 2022. Between July 2022 and June 2023, around four million people in the

UK reported having used Generative AI tools for work,¹ and 8% of EU companies report using AI to perform at least one function of their business.² While the narrative around AI is regularly dominated by industry experts, focussing on its potential for the economy, little attention is given to the harms that it is already inflicting on people at the coalface. In the UK alone, there is evidence that AI facial recognition replicates existing biases and discriminates against racialised groups;³ artists, writers and musicians are

- 1 <https://www2.deloitte.com/uk/en/pages/press-releases/articles/more-than-four-million-people-in-the-uk-have-used-generative-ai-for-work-deloitte.html>
- 2 <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240529-2>
- 3 <https://www.bbc.co.uk/news/technology-68655429>



worried about copyright infringement by data scraping AI tools while pushing for new legal restrictions that may harm researchers and other public goods,⁴ and disabled people are unfairly targeted by AI tools used by the Department for Work and Pensions.⁵ ORG will need to monitor, investigate and challenge harmful applications of AI and policy responses, particularly regarding immigration, criminal justice, privacy and free expression, before they become deeply rooted.

There was continued media and political exploitation of Europe's migrant crisis and the arrival of people seeking asylum in the UK via small boats. The hostile environment for migrants continues to impact the digital rights of some of the most marginalised and vulnerable people in our society.

Towards the end of the reporting year, the Palestinian militant group Hamas, which controls the Gaza strip, launched an attack on Israel, killing over 1,200 people and taking hundreds more hostage. Almost immediately, Israel responded with military action, which at the time of writing this report has killed over 34,000 people, a third of whom are children.

The escalation of the war and the humanitarian crisis in Gaza is impacting global politics and testing freedom of expression in countries around the world, including the UK. Within days of the Hamas attacks, the then-Home Secretary had written to police chiefs suggesting that certain chants and even waving a Palestinian flag could be seen as crimes. The Education Secretary wrote to schools reminding them of their duties under Prevent. Several ministers spoke of revoking the visas of migrants who were seen to support Hamas. The political response to the crisis has threatened freedom of expression in the UK.

Internally, ORG worked on its culture and teamwork as an organisation, engaging consultants to gather feedback from our team and review our practices. We will continue to work on this, to ensure that ORG is an effective organisation, able to react to the demands of a shifting digital rights landscape and well-positioned to highlight the experiences of those most impacted by digital harms.

4 <https://techmonitor.ai/technology/ai-and-automation/will-2023-be-year-of-ai-lawsuit>

5 <https://www.foxglove.org.uk/2021/12/01/secret-dwp-algorithm/>



COMBATING BIG TECH AND PLATFORM POWER

Privacy and data protection

In a world that is increasingly embracing AI and other novel technologies, existing safeguards for privacy and data protection should be strengthened, not weakened. ORG continued to defend strong data protection laws, helping the public to keep themselves safe from crime, abuse and exploitation. We also continued to hold organisations to account within a data ecosystem that prioritises governments and big corporations.

Data Protection and Digital Information Bill

We continued our fight against the Data Protection and Digital Information (DPDI) Bill. We have consistently argued that the bill weakens data subjects' rights and corporate accountability mechanisms, lowering the threshold for organisations to refuse a Subject Access Request (SAR) and removing individuals' right to not to be subjected to wholly automated decision making. The Bill also reduces the independence of the Information Commissioner's Office (ICO), expands the grounds for processing data, and gives the Secretary of State discretion to approve international data transfers to countries with insufficient data protection standards.

In March 2023, ORG organised an open letter, signed by 26 civil society organisations, to the Secretary of State for Science, Innovation and Technology, Michelle Donelan MP, calling for the DPDI Bill to be dropped. The signatories include trade unions as well as human rights, healthcare, racial justice, migrants' rights, workers' rights and criminal justice organisations. They are concerned that the government's proposals

will seriously weaken data protection rights in the UK, and could particularly harm people from marginalised communities.

Ahead of the second reading of the DPDI Bill in the House of Commons, we published our Parliamentary briefing for MPs. Our briefing was quoted four times during the Parliamentary debate by representatives of the Labour Party, Liberal Democrats and the Scottish National Party. We set out how changes to GDPR law mean the government is setting the country on a dangerous path that weakens individuals' data protection rights and corporate accountability mechanisms, as well as giving the government undemocratic powers.

The right to access personal information hit the news when Nigel Farage submitted a SAR to find out why Coutts bank had closed his account. We used this opportunity to highlight our concerns, which resulted in a Guardian article about the impact of the Bill.⁶

The threats posed by the Bill were also highlighted by major data breaches involving the Electoral Commission and the Police Service of Northern Ireland.⁷

Adequacy agreement

ORG had previously briefed members of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament about the DPDI Bill and our concerns for the data rights of European citizens.⁸

Throughout the year and as the Bill made its way through Parliament, ORG kept briefing several MEPs across the EU political spectrum, as well as DG Connect and the EU Representation in London, to raise awareness about the impact of the Bill on UK data protection standards. This included our presentation, in July 2023, at the event

“Common futures, different rules? The new EU – UK relationship”, with a focus on regulatory divergence in the data protection field.

In July 2023, 28 civil society organisations wrote to the European Commission warning that the DPDI Bill would turn the UK into a ‘leaky valve’ that would undermine the data protection rights of European citizens.⁹

AI regulation

Throughout the year, ORG led and participated in many conversations about the impact of AI on different areas of society. In December 2022, we participated in an AI Workshop convened by the Competition and Markets Authority to discuss competition issues in the AI field, which fed into their ongoing investigation of Foundation Models.¹⁰ ORG also joined a roundtable convened by the Law Society on AI and access to Justice, resulting in a report on challenges to the justice system, including the risks posed by AI in a justice context.¹¹

Towards the end of this financial year, ORG convened a joint letter with Connected by Data and the Trade Union Congress that criticised the Government’s approach to AI safety, including its closed-door AI Safety Summit.¹² The contents of that letter were reflected in US Vice-President Kamala Harris’ address to the summit.¹³ In response to the exclusion of civil society actors from the event, ORG organised a session at the civil society-led AI Society Forum, where we platformed the voices of people from racialised and overly-surveilled communities already experiencing the harms of AI in policing, counter-terrorism and immigration contexts.¹⁴

⁶ <https://www.theguardian.com/technology/2023/aug/06/uk-data-bill-favours-big-business-and-shady-tech-firms-rights-group-claims>

⁷ <https://www.openrightsgroup.org/press-releases/uk-shaken-by-major-data-breaches-security-concerns-surge-over-data-protection-changes/>

⁸ <https://www.openrightsgroup.org/blog/the-uk-data-protection-reforms-from-an-eu-perspective/>

⁹ <https://peoplevsbig.tech/open-letter-to-the-eu-commission-regarding-uk-s-data-bill>

¹⁰ <https://www.gov.uk/cma-cases/ai-foundation-models-initial-review>

¹¹ <https://www.lawsociety.org.uk/campaigns/21st-century-justice>

¹² <https://ai-summit-open-letter.info/>

¹³ <https://www.nytimes.com/2023/11/01/us/politics/kamala-harris-ai.html>

¹⁴ <https://www.aisocietyforum.net/>

Adtech

In 2023, our focus shifted toward online advertising practices of new identity resolution systems – in other words, a new form of online tracking that relies on either first-party cookies or offline identifiers. Following intense regulatory pressure and Google's decision to deprecate third-party cookies,¹⁵ the online advertising industry has tried to roll out new online tracking mechanisms that fall short of protecting users' privacy and do not address the issue we had identified with our adtech complaint in 2018. ORG also worked in partnership with complainants from France and CrackedLabs¹⁶ to lay the groundwork for a new complaint against these systems.

UK ICO

In 2023, ORG submitted three SARs to LiveRamp, the responses to which evidenced that we had suitable candidates for complainants in the UK. We then filed a complaint with the ICO, despite the new internal policy adopted by the new Information Commissioner requiring complainants to engage with controllers before lodging a formal complaint with the ICO.¹⁷ As this project seeks to promote an investigation into LiveRamp's practices and to resolve data protection infringements systemically, we did not want to give LiveRamp the option to address our concerns on an individual basis while leaving its data practices unaltered and failing to address the systemic risks they present. Furthermore, if the ICO drops our complaint on these grounds, it would demonstrate a divergence in how EU data protection laws are applied across jurisdictions.

France and the United States

Within this project, we collaborated with La Quadrature du Net to file parallel complaints in France. La Quadrature is well-

known and has an established relationship with the CNIL, France's data protection authority, and with their involvement we hope to raise the chances that our complaint is taken seriously in France.

Campaigning

Accompanying our litigation efforts, we increased the pressure on the ICO via campaigning activities. Our campaign highlighted that the ICO's engagement with the adtech industry has left us with a worse situation than before, and that the EU has, in contrast, taken regulatory action to contest the adtech space. Failure of the ICO to act upon this complaint could be leveraged to raise broader criticism around the institutional direction the ICO are taking, with the aim of resisting such changes and, in the future, promote positive reform.

Data and democracy

Since 2018, ORG has been investigating the misuse of data by political parties. This year, we built on this work and on investigations led by other organisations by exploring the use of apps by the parties. The objective of our investigation was to explore whether the apps themselves and the companies that produce them offer investigative leads, to help uncover which companies operate on behalf of the political parties to segment voter data obtained via canvassing.

We have undertaken significant research into how political parties in the UK trade and grade the personal data of voters for their own electoral benefit. We also commissioned an external researcher to undertake a forensic examination of the apps, including what data is collected about individuals by canvassers, and how that data is sent from apps to political parties and others. Having raised the alarm previously about the influence of Experian as a provider widely used by the political parties, we also wanted to identify, in more detail, the role Experian and other data brokers play. We will be building on this research in light of the election in the coming year, ensuring that voters are aware of their digital rights when engaging with political canvassers and campaigning to improve the data protection policies of all the main parties.

¹⁵ <https://www.forbes.com/sites/forrester/2024/01/16/google-commits-to-third-party-cookies-deprecation-in-2024/>

¹⁶ <https://crackedlabs.org/en>

¹⁷ <https://ico.org.uk/make-a-complaint/data-protection-complaints/what-to-expect/>

CHALLENGING STATE INTRUSION INTO RIGHTS ONLINE

ORG is working to challenge general monitoring and state censorship of online content, speech regulation and the chilling effects of government mass surveillance.

Protecting freedom of expression online

Online Safety Bill

ORG continued to advocate against and campaign on the Online Safety Bill, raising awareness of the threat it poses to freedom of expression and privacy online. Many clauses in the Bill would amount to 'prior restraint' - that is, the interception, blocking or removal of content before it is published on the platform. There are a number of issues with prior restraint, namely that AI- driven systems make mistakes because these systems are blind to context and intention, and "false flags" are common. Moreover, online platforms are likely to be overcautious as the Bill mandates harsh consequences for non-compliance, including criminal liability and even jail time. Our concern is that the Bill could silence legitimate speech, shutting down public debate.

In May 2023, ORG held an online roundtable to discuss the proposals under the Bill that control expression and constitute a form of censorship. Participants came from across the spectrum of civil society, including representatives from groups working on over-policing, youth justice, counter- terrorism, and women's and migrants' rights. The event was chaired by Dr Monica Horten, Policy Manager (Freedom of Expression), who also briefed participants on the unintended consequences of prior restraint and the mechanism for removing illegal content.

Following the roundtable, ORG received legal advice from Dan Squires KC and Emma Foubister of Matrix Chambers, which states that measures in the Online Safety Bill may involve breaches of international law.

The legal opinion confirms ORG's position that Clause 9(2) of the Bill "amounts to prior restraint", by placing a duty on online platforms, such as Facebook and Twitter, to prevent users from "encountering" certain "illegal content". It will require platforms to screen, intercept and block online communications before they have been posted. This, the opinion warns, represents, "a sea change in the way public communication and debate are regulated in this country" as people may be censored before they have even been able to post online.

ORG and EFF published a joint briefing which outlined the harms of age verification proposals within the Bill.¹⁸ The Bill required sites that allow user-generated content, such as Facebook, Tik Tok and even Wikipedia, to prevent children from seeing content the government has defined as 'harmful'. This could present platforms with the choice of sanitising their sites so that all content is considered suitable for children or asking users to verify their ages through government-issued documents or by using biometric data, such as face scans, to estimate ages.

The Bill was finally passed in September 2023. ORG warned that it will make us less secure by threatening our privacy and undermining our freedom of expression. This includes damaging the privacy and security of the children and young people the law is supposed to protect.¹⁹

¹⁸ <https://www.openrightsgroup.org/press-releases/online-safety-bill-us-and-uk-campaigners-warn-of-dangers-of-age-verification/>

¹⁹ <https://www.openrightsgroup.org/press-releases/org-warns-of-threat-to-privacy-and-free-speech-as-online-safety-bill-is-passed/>

Blocked.org.uk

Mobile and broadband Internet Service Providers (ISPs) have created filters to stop under-18s from seeing harmful content online. Unfortunately, filters block many harmless websites by mistake – even sites that are aimed at children. Often website owners need to learn that this is happening.

Our Blocked.org.uk tool continued to help users find out if a website is blocked by their Internet service provider, by mobile content filters or by a court-ordered block. Our service also helped users file requests to get sites unblocked.

Fighting the surveillance state

Encryption

As part of our fight to defend end-to-end encryption, we participated in regular outreach and engagement with members of the Global Encryption Coalition, entailing joint actions and briefing members on policy research.

In November 2022, ORG was one of 70 organisations, cyber security experts and elected officials (all members of the Global Encryption Coalition) who signed an open letter to Prime Minister Rishi Sunak on the need to maintain the security of E2EE. Our Policy Manager also presented to Coalition members on what the Online Safety Bill could mean for the security of E2EE in both the UK and global context. This was followed by the publication of an in-depth policy briefing entitled, 'Who's Checking in on your chats in private online spaces?' The briefing was shared across ORG's communication channels and with our partner network.

In 2023, we partnered with 89up to produce a campaign video²⁰ for the 'Don't Scan Me' campaign against the spy clause in the Online Safety Act that exposes our private messages to mass surveillance. The spoof video of a phone inspector, played by comedian Ali Woods, asking the public to hand over their phones has been viewed 1.6K times on YouTube.

We took to the streets of London with a digital display van that raised awareness of the encryption- busting message scanning

powers in the Bill. We were joined outside Parliament by ORG supporters and Alistair Carmichael MP, Liberal Democrat Home Affairs, Justice and Northern Ireland spokesperson.

We continued to raise awareness throughout the year, promoting the protection of end-to-end encryption with the general public, CSOs and MPs.

ORG and the pan-European network of over 47 organisations, European Digital Rights (EDRi), co-ordinated a letter to the UK government signed by over 80 civil society organisations, academics and cyber experts from 23 countries.²¹ The letter warned that message-scanning proposals in the Online Safety Bill could make chat platforms insecure for everyone.

In September, ORG hosted a meeting in Parliament with a wide range of civil society groups. At this meeting, colleagues from Amnesty International, Stonewall, Liberty, Big Brother Watch, EFF, Article 19, Citizen Lab and the not-for-profit Signal Foundation all spoke out about the problems with breaking end-to-end encryption. These partners talked movingly about the genuine threat that the Government's proposals pose to LGBTQIA+ people, human rights defenders and journalists worldwide.

ORG raised awareness of the threat to encryption through media work, and our commentary was featured in articles by the BBC, Guardian, Politico, New Statesman, Computer Weekly and other tech outlets. We welcomed shared concerns by tech companies, including Signal, WhatsApp and Element.²²

During the final discussion and votes on the Online Safety Bill, the government conceded that it will not use powers to scan private messages until it is "technically feasible" to do so. While this admission that it could not scan messages safely was a victory, the powers remain on the statute book.²³

²⁰ <https://www.youtube.com/watch?v=oGvmeFweHnA>

²¹ <https://www.openrightsgroup.org/press-releases/online-safety-bill-protect-encrypted-messaging/>

²² <https://www.openrightsgroup.org/press-releases/whatsapp-signal-and-element-online-safety-bill-poses-an-unprecedented-threat-to-the-privacy-safety-and-security-of-every-uk-citizen/>

²³ <https://www.openrightsgroup.org/press-releases/government-admits-spy-clause-cant-be-used-safely/>

Keeping Surveillance out of green technology

On 1 October 2022 the Government quietly announced that smart meter data would be collected in order to assess the bills reduction scheme following the energy price hikes of 2021. The changes were flagged in privacy policies and were unaccompanied by any details or explanation of exactly why the data was being collected or how it would be used.

ORG raised the alarm: this broke promises made for many years that government would not attempt to seize smart meter data. Smart meter data can reveal intimate details about people's personal lives, revealing exactly when they are at home and the type of activities they are engaging in and appliances they are using. Furthermore the government asked to keep this data for 'as long as required' or up to ten years.

We wrote to the government in December to ask for clarity and continued to follow up with them. Their response failed to properly address our questions about data protection impact assessments (DPIAs), transparency, consent and the amount of personal data that would be collected. ORG maintained the pressure, engaging with the government and relevant authorities.

Finally, in April 2023, the government announced that they were reducing the detail of the data they intend to collect.²⁴ Data will now be collected on a monthly basis and the related privacy notice draws attention to individuals' right to object. However, in August, the government amended this guidance to state that "in line with the Data Access and Privacy Framework, energy consumption data is being collected more frequently than monthly".²⁵

²⁴ <https://www.gov.uk/government/publications/energy-price-guarantee-scheme-privacy-notice/use-of-electricity-meter-and-gas-meter-personal-data-collected-through-the-energy-price-guarantee-scheme-privacy-notice>

²⁵ <https://www.gov.uk/government/publications/energy-price-guarantee-scheme-privacy-notice/use-of-electricity-meter-and-gas-meter-personal-data-collected-through-the-energy-price-guarantee-scheme-privacy-notice>

DIGITAL THREATS AGAINST COMMUNITIES MADE VULNERABLE BY SOCIETY

Migrant Digital Justice Programme

Since 2020, ORG has worked to understand the needs and capacities of civil society organisations working in the field of migrants' rights and to support them to incorporate digital advocacy into their work. This work to expose and challenge the digitisation of the UK government's hostile environment policy was brought under a new umbrella, the Migrant Digital Justice Programme, in early 2022.

Network

Over the past year, ORG has continued to grow its network of migrants' rights partners through outreach, events and ongoing collaboration. Since the inception of this programme, ORG has worked with 39 migrants' rights groups and has reached nearly 200 subscribers through its newsletters. This networking has helped us form a number of new and fruitful partnerships, collaborating in different ways on distinct issues.

We continue to engage with migrants' rights groups at a grassroots level and facilitate events and communications through our local groups, including by working with individual activists and supporters in target cities. Many of the digital rights campaigners already in our network are interested in the specific challenges faced by migrants, while activists in the migrant sector have been encouraged to join local ORG chapters. This reinforces support for campaigns at the intersection of digital and migrants' rights.

Refugee Week

2023 marked the 25th anniversary of 'Refugee Week', which we joined for the first time, promoting the week across our channels as a way of reaching new migrant communities and migrants' rights organisations. As part of Refugee Week, we shared seven tips for refugees and migrants to exercise digital rights effectively in the UK,²⁶ visited over 100 times, and translated into Farsi, Arabic and Ukrainian, as well as an article critiquing the digital hostile environment that targets migrants. We will continue to mark Refugee Week in the coming years, given how it helped raise our profile with new groups in ways that otherwise would not have been possible, with organisations reaching out proactively to us for support.

Migrant Perspective on DPDI Bill

ORG published a briefing to MPs about how the DPDI Bill will harm migrants' data rights, with 22 organisations signing on.²⁷ We have run a series of events and panels to raise awareness of the flaws in this Bill with migrants' rights groups and those serving migrants, including an online event.²⁸ Our blog on the surveillance that the DPDI would allow of bank accounts has been read over 700 times.²⁹ We also continue to mobilise support with the public, policymakers and MPs, with our briefing quoted four times during the Parliamentary second reading debate by representatives of the Labour Party, Liberal Democrats and the Scottish National Party.

²⁶ <https://www.openrightsgroup.org/refugee-week-digital-rights-tips/>

²⁷ <https://www.openrightsgroup.org/app/uploads/2023/05/DPDI-Bill-Briefing-on-Migrants-Rights.pdf>

²⁸ <https://www.youtube.com/watch?v=0Qllerftlb8>

²⁹ <https://www.openrightsgroup.org/press-releases/dpdi-bill-new-welfare-surveillance-proposals-target-vulnerable-people/>

Challenge the Checks

In collaboration with Migrants at Work and the Migrants' Rights Network, we continue to develop our campaign on the digitalisation of 'right to work' checks.³⁰ The digital right to work checks are hugely flawed, with widespread issues with false negatives and errors in the system that leave many migrants without work and at risk of destitution. ORG joined two APPGs this year about modernising and digitalising employment in the UK. During this session, we raised our concerns regarding the right to work checks, which reinforce discrimination against the most vulnerable groups in the UK.

Alongside the ongoing campaign, we are reaching the end of our evidence gathering stage, which has amassed case studies and witness statements from hundreds of migrants, refugees and asylum seekers with lived experience, and experts across the sector. It is our ambition to launch a legal challenge of the digitalised right to work checks, either focused on their perpetuation of discriminatory decision-making, or arguing that there is no mechanism through which migrants can seek recourse for incorrect or out of date data held on them.

Pre-crime, data and technology

The Pre-Crime Programme pilot at ORG was developed in response to worrying trends in the ways digital "innovations" are being used by law enforcement and counter-terrorism agencies to weaponise data. Social media content and personal data are being collected, shared and retained to make tenuous links to crimes and to predict susceptibility to violence, in some cases before a crime has even been committed. In collaboration with racial justice and community groups, we have been developing this work, investigating, documenting and challenging abuses to digital rights across policing and counter-terrorism.

³⁰ <https://migrantsrights.org.uk/projects/challenge-the-checks/>

Investigating the Digital Harm of the Prevent Duty

A narrative around “suspect” behaviour and “preventing” terrorism before it happens culminated in the UK’s Prevent Duty, whereby public authorities, such as doctors, teachers and social workers, have a duty to report what they believe suggests radical behaviour or vulnerability to radicalisation.

We responded to the Shawcross review of Prevent, which failed to address multiple problems with Prevent, including its chilling effect, the danger of driving radical discourse underground, misconceptions around faith and identity, and ignorance of the ripple effect a referral can have on someone’s life.³¹

Throughout 2023, we conducted an in-depth investigation into how Prevent referrals were made and shared with different agencies - the first of its kind. With support from Prevent Watch, the key watchdog on Prevent, and researchers Lewis & Klein Associates, we sought to explain how personal data is collected, retained and shared under Prevent and how this processing meets data protection standards.

Together we conducted a comprehensive online search of publicly available information, followed by FOI requests to authorities in England and Wales. Our findings are based on 56 disclosures, which provide a snapshot of how the government, the police, local authorities, universities and the NHS share data when making referrals under the Prevent Duty. Despite the challenges that come with investigating counter-terrorism, including navigating the use of national security exemptions provided by the Freedom of Information Act, we made a number of alarming discoveries that formed the basis of a report launched in 2024.

Police Surveillance

ORG is working to expose and challenge the impact of surveillance on communities that are disproportionately targeted by measures such as social media weaponisation, live facial recognition software and police databases. The police’s increasing reliance on the monitoring of associations, musical taste and social media activity to determine the likelihood of committing violence constitutes a digitalised form of racial profiling.

ORG joined other groups in the sector to explore options for collective action on issues such as Project Alpha (the collection by Police of “children’s personal data” from social media sites), live facial recognition technology and the use of ANPR by police. We also collaborated with grassroots racial and social justice organisations to develop a “Know Your Rights” toolkit, which will form the basis of a training to empower youth workers and young people to challenge abuses of their digital rights in the new year.

Challenging Gang Narratives

In March 2023, we published our open letter to the Mayor and Chief Constable of Greater Manchester.³² Joined by 14 other civil society groups, we highlighted the injustice of the conviction of ten young Black boys known as the Manchester 10. The case shines a light not only on the flawed offence of joint enterprise but also the use of music lyrics as evidence of criminal intent, even when a crime hasn’t been committed. Sophia Akram, former ORG Programme Manager, notes that this is part of a wider practice where “police forces are mining the social media accounts of young people, in order to identify them as gang members. This creation of ‘gang narratives’ based on musical expression disproportionately impacts Black men.”

³¹ <https://www.openrightsgroup.org/press-releases/open-rights-group-responds-to-shawcross-review-of-prevent/>

³² <https://www.openrightsgroup.org/press-releases/end-racialised-surveillance/>

GRASSROOTS COMMUNITY, MEMBERSHIP AND ACTIVISM

There were two Parliamentary bills passing through Parliament during this period: the Online Safety Act and the Data Protection and Digital Information (DPDI) Bill. These were the main focus of our activist activities.

In October 2022, we launched our "Hands Off Your Data" campaign around the DPDI Bill. This initiative prompted over 750 people to write to their MPs about the bill. We produced a 'Stop the Data Discrimination Bill' leaflet³³ that was used by groups to raise awareness of threats posed by the DPDI Bill amongst delegates at the major political party conferences. We also produced a film about this on YouTube and Facebook.³⁴ The campaign included a downloadable pack for people to use to take action in groups.

Our other major campaign focused on the Online Safety Act. In July 2023, this crowdfunded campaign saw activists gather in London with a video van, and featured online advertising videos as part of the "Don't Scan Me" campaign. Over 1,100 people supported this action, engaging in activities to lobby both MPs and Lords. This campaign culminated in an intervention in the Lords at a briefing event hosted by ORG, which collaborated with Signal, Amnesty, Big Brother Watch, and EFF to secure concessions from the Government regarding the scanning of private messaging apps.

We also participated in several in-person events. We held a stall at the Green Party Conference on Migrants' Digital Rights, maintained a presence outside both the Labour and Lib Dem spring conferences, and had stalls at some regional party conferences.

Despite the challenges of group activity post-COVID, Manchester ORG held an event in the summer of 2023. Additionally, we successfully launched an advocacy volunteer scheme, with two groups of individuals participating in online training on how to advocate for digital rights issues.

Furthermore, we developed a new ORG leaflet and pop-ups for these in-person events. We also hosted petitions on platforms such as Care2, which provided us with new sources of contacts.

Our online activism expanded to new platforms with the launch of our TikTok channel during this period. This is an essential part of our effort to engage the next generation of digital rights activists and campaigners. Our film on the passing of the Online Safety Bill had over 113k views.

Approved by the board on 09/07/2024


Christian Scarborough, Director

³³ <https://www.openrightsgroup.org/publications/stop-the-data-discrimination-bill-leaflet/>

³⁴ <https://www.youtube.com/watch?v=iC5RdnCstH8&t=36s>

INCOME AND EXPENDITURE ACCOUNT

for the year ended 31 October 2023

	NOTES	2023 £	2022 £
INCOME			
Gifts and donations income		(13,483)	19,672
Business membership		7,547	15,973
Grants	6	570,902	421,435
Supporter donations		172,613	181,509
Public event income		40	-
Profit / (Loss) on asset sales		(114)	-
		737,505	638,588
EXPENDITURE			
Accounting and other professional fees		5,680	9,975
Associations and memberships		6,060	5,255
Bank charges		383	216
Contractors and specialists		9,546	1,650
Depreciation		5,223	4,079
Donation processing charges		9,711	9,855
Foreign exchange losses / (gains)		551	(3,523)
General campaigning		94,846	86,640
Grants made		2,778	2,925
Insurance		2,268	1,814
Office supplies		3,498	2,180
ORGCon and public event costs		159	(200)
Other expenditure		1,146	(3,479)
Postage and printing		976	543
Rent and rates		2,674	1,809
Salaries		515,637	369,994
Service providers		26,941	14,660
Staff recruitment		4,206	16,654
Staff training		9,107	10,300
Strategic litigation		2,655	34,298
Strategy and planning		20,907	9,479
Travel and subsistence		6,277	2,475
Website costs		330	406
		731,557	578,007
Surplus of income over expenditure for the year		(1,052)	60,580
Balance brought forward		144,113	83,532
Balance carried forward		143,061	144,113

BALANCE SHEET

for the year ended 31 October 2023

	NOTES	2023 £	2021 £
FIXED ASSETS			
Tangible Assets	4	8,701	11,017
CURRENT ASSETS			
Prepayments		7,272	7,025
Staff loans	5	23	101
Grants receivable		2,100	2,360
Other debtors		0	294
Cash at bank		706,657	405,262
		716,052	415,042
CREDITORS: AMOUNTS FALLING DUE WITHIN ONE YEAR			
Creditors		10,807	6,680
Funding received in advance		551,760	258,549
Other creditors		19,125	16,717
		581,692	281,946
Net Current Assets		134,360	133,096
Net Assets		143,061	144,113
CAPITAL AND RESERVES			
Profit and loss		143,061	144,113
ACCUMULATED FUNDS			
		143,061	144,113

A copy of ORG's official accounts is available on request from info@openrightsgroup.org

NOTES TO THE ACCOUNTS

for the year ended 31 October 2023

1 Accounting policies

Basis of preparation of financial statements

The accounts have been prepared under the historical cost convention and in compliance with FRS102 Section 1A as it is applicable to the financial statements for the period. There were no material departures from the reporting standard.

2 Surplus income and the Accumulated Fund

As a not for profit company, all income is dedicated to its object of raising general awareness of digital rights matters and is credited to an accumulated fund to be used for future projects. As a company limited by guarantee and without share capital, income cannot be distributed to shareholders.

3 Supporter Donations

Regular supporter donations are treated on a cash basis, i.e. are treated as pertaining to the month in which they are received.

4 Tangible Fixed Assets

Depreciation has been provided at the following rates in order to write off the assets over their useful economic lives:

Office Equipment: 33% straight line

	OFFICE EQUIP. £
COST OR VALUATION	
At 1 November 2022	27,668
Additions	4,208
Disposals	(3,608)
	28,268
DEPRECIATION AND IMPAIRMENT	
At 1 November 2022	16,651
Charge for the year	5,223
Disposals	(2,307)
	19,567
NET BOOK VALUE	
At 31 October 2023	8,701
At 31 October 2022	11,017

5 Staff Loans

Staff loans are extended typically for the purchase of season tickets, and are repaid by equal deductions from the employees' salaries.

	2023	2022
Average number of employees during the year	10	9

6 Grant income

	2022 £	2021 £
Avast	-	14,705
Borja	-	760
Digital Freedom Fund	33,491	33,917
Duck Duck Go	19,966	-
Heinrich Boll Foundation	-	11,130
Internet Society	16,305	31,695
Investment Fund	18,259	-
Joseph Rowntree Reform Trust Ltd	38,498	-
Oak Foundation	122,441	88,116
Open Society Foundations	187,723	144,811
Paul Hamlyn Foundation	59,605	56,171
PIA Income	-	100
Reset	74,614	40,030
	570,902	421,435



