DEMOS

ADVANCING DIGITAL RIGHTS IN 2025

TRENDS, CHALLENGES, AND OPPORTUNITIES IN THE UK, EU AND GLOBAL LANDSCAPE

HANNAH PERRY
SUMAYA NUR ADAN
NAEMA MALIK
SOPHIA KNIGHT

In partnership with

AI GOVERNANCE INITIATIVE
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD

FEBRUARY 2025

Published by Demos February 2025

15 Whitehall, London, SW1A 2DD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk

CONTENTS

ACKNOWLEDGEMENTS

We would like to thank all those who contributed to our research, including representatives from government, regulators, digital rights organisations and academics who participated in our interviews, roundtable and workshop discussions. We would particularly like to thank representatives from the following organisations who generously shared their time and expertise:

- 5 Rights Foundation
- Ada Lovelace Institute
- Access Now
- AI Now Institute
- Amnesty Tech
- Awo Agency
- Big Brother Watch
- Dr Igor Calzada, Cardiff University
- Centre for Democracy and Technology
- Dr Elinor Carmi, City University
- Connected By Data
- Centre for Countering Hate
- Digital Poverty Alliance
- Equality Now and The Alliance for Universal Digital Rights (AUDRi)
- Good Things Foundation
- Green Web Foundation
- Hogan Lovells
- Information Commissioner's Office
- Institute for Strategic Dialogue
- Institute for Government
- Internet Watch Foundation
- James Ball, Demos Fellow
- Dr Bart Custers, Leiden University
- Nominet
- Ofcom
- Online Safety Act Network
- Open Future Foundation
- Open Rights Group
- People vs Big Tech
- The Royal Society
- Dr Birgit Schippers, Uni. of Strathclyde
- Dr Meg Davis, Uni. of Warwick
- Renan Araujo, Institute for AI Policy & Strategy
- Juliana Martins, Faculty of Law, University of Oxford
- Luise Eder, Centre for Socio-Legal Studies

This report was produced by Demos, in collaboration with the Oxford Martin School AI Governance Initiative, and is editorially independent. Any errors are the authors' own.

We would like to thank the generous support of the Government of the Republic of South Korea who funded this work between August and December 2024.

Thank you also to our colleagues for their input and support at various stages throughout this project: Elizabeth Seger, Robert Trager, Bessie O'Dell, Andrew Phillips, Polly Curtis, Jamie Hancock, Sumaya Akthar, Chloe Burke and Aidan Garner.

Hannah Perry
Sumaya Nur Adan
Naema Malik
Sophia Knight

February 2025

ABOUT THIS REPORT

Demos is Britain's leading cross-party think tank. We put people at the heart of policy-making to create bold ideas and a more collaborative democracy.

This paper is part of Demos' strategic focus area on '***Trustworthy Technology***'. With emerging technologies transforming our world at an ever-faster pace, we work to build bridges between politicians, technical experts, and citizens to explore solutions, improve trust, and create policy to ensure technological progress aligns with the needs and values of citizens.

This paper is co-authored with the Oxford Martin School AI Governance Initiative which aims to understand and anticipate the lasting risks from AI through rigorous research into the technical and computational elements of AI development, combined with deep policy analysis.

This report was funded by the Government of the Republic of South Korea following the publication of its Digital Bill of Rights. Our work remains editorially independent.

EXECUTIVE SUMMARY

BACKGROUND

Historically, policymakers globally have struggled to balance protecting citizens' rights with enabling a flourishing technology industry to fuel economic growth and innovation. Yet, there are new tools at policymakers' disposal. Whilst strongly divergent priorities have emerged between China, the USA and Europe, across the world, we are observing an evolution of human rights norms and discourse surrounding 'digital rights'.

In the last two years, digital rights have found form in national and regional instruments exemplified by the European Union's Declaration of Digital Rights and Principles as well as South Korea's recent Digital Bill of Rights. Such instruments provide a holistic framework of digital rights to guide legislative, policy, and technological development. In 2024, as the United Nations commits to a Global Digital Compact, this trend inspires some hope for more forward thinking and globally joined-up policymaking that protects and enables the basic rights of citizens in a digital world in 2025.[1,2]

In this context, Demos, in partnership with the Oxford Martin School AI Governance Initiative, and supported by the Government of the Republic of South Korea has explored the definitions, trends, challenges and new possible approaches to advancing digital rights in the UK and EU.

This paper follows a literature review, a series of expert interviews, a roundtable and a workshop with EU and UK digital rights organisations, academics and policymakers.

DEFINING 'DIGITAL RIGHTS'

The definition of 'digital rights' is fluid - reflecting a mishmash of legal frameworks ranging from fundamental human rights declarations to data protection, cybersecurity, consumer rights and copyright legislation - evolving in the hands of different digital rights movements submerged in different political, social and legal contexts.[3] At a high-level, digital rights include both an extension of existing fundamental human rights into the digital world, such as the right to freedom of expression and information in a digital environment, *and* wholly new rights, such as the right to digital access or participation in technological development.

1 United Nations (2024) Global Digital Compact. https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf

2 Denardis (2020) The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press https://doi.org/10.2307/j.ctvt1sgc0.

3 Warso (2023) Digital Rights Revisited https://openfuture.eu/wp-content/uploads/2023/10/231017Digital-rights-revisited.pdf; Postigo (2012) "The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright", The Information Society Series 7

TRENDS

Over the last twenty-five years, there have been six broad waves of digital rights-related governance at the UK, EU and global level, some of which overlap and two that are newly emerging and ongoing.

1. **A foundational global wave** at the international governance level began in the early 1990s sowing the seeds for digital rights with a focus on digital access and freedom of expression;
2. **A privacy wave** across Europe running to the mid-2010s with the resulting General Data Protection Regulation (GDPR) is now recognised as the global data protection standard;
3. **A diversification wave** with greater consideration of a wider range of rights into the late 2010s, including advocacy for stronger protections for freedom of expression, non-discrimination and children's rights in the digital world informed the development of the EU's Digital Services Act and UK's Online Safety Act.
4. **A preventative wave** with emphasis on rebalancing the power and influence of technology companies relative to other industries, is exemplified by the EU's Digital Markets Act and the UK's Digital Markets, Competition and Consumers Act.
5. **A decolonising wave** within the European digital rights movement has created new space for understanding the concerns of communities most affected by digital rights abuses, including in the context of migration, economic and climate justice.[4]
6. **A democratisation wave of new global principles**, exemplified by the UNESCO's Recommendation on the Ethics of AI, their AI Readiness Assessment and the Global Digital Compact, collectively normalise new rights ranging from algorithmic accountability to equitable access to AI resources. Conceptions of digital access are also now evolving to include participation in technological development, requiring recognition of the crucial role of basic, critical and advanced digital literacies.

These latter two new, overlapping waves of decolonisation and newly emergent global principles reflect fresh opportunities for UK and EU digital rights activists and policymakers to build from.

CHALLENGES

UK and EU rights advocates highlighted a number of pre-existing challenges with advancing digital rights. Of course, the European and UK contexts are very different, particularly with regards to socio-cultural norms surrounding human rights. This is symbolised by the fact that the EU has already launched a Declaration of Digital Rights and Principles, while the UK lacks one. Yet there are common themes.

Both the EU and UK digital rights advocates highlight:

1. An 'uneven playing field' when describing their ability to advocate for digital rights to states in relation to their technology industry counterparts. Digital rights organisations are unable to match the resources of technology companies to influence legislation.
2. Digital rights advocates struggle to articulate convincingly that stronger digital rights protections are not in tension with economic growth and innovation.
3. States are frequently making exemptions to their protections of digital rights in legislation to empower law enforcement and border control. Such loopholes contravene the fundamental principle of human rights being applicable to all equally.

4 EDRi (2024) "Decolonising Digital Rights." https://edri.org/what-we-do/decolonising-digital-rights/

4. Legislative efforts too rarely take approaches for enforcement and redress into account in their development. As a result, enforcement of existing technology-focused laws, such as the GDPR, is felt to be poorly resourced and insufficient. There are also significant concerns regarding the lack of routes for redress for citizens who experience such harms exacerbated by their low awareness of the opportunities to do so. Both limitations devalue the power of the legislation to sufficiently protect citizens.
5. There are insufficient protections for societal harms such as the impact of technology on democratic systems and the environment. There needs to be greater consideration and policy development to tackle these crucial areas.

UK digital rights advocates in particular also highlighted that:

6. There are currently insufficient protections and routes to redress for collectives such as minority ethnic communities or workers despite there being distinct harms that can be exacerbated by technologies that affect such groups, such as algorithmic bias or workplace surveillance.
7. There is a lack of coordination and joined up advocacy within the UK digital rights movement which is resulting in different digital rights organisations advocating for protections and goals in a siloed way, that can clash and produce corresponding infringements in the final negotiated legislation. This was exemplified by the outcomes of the Online Safety Act which included a number of provisions which satisfied some digital rights advocates, but represented infringements on rights for others.
8. Digital access and skills whilst a key policy area and priority for digital inclusion charities in the UK is not currently conceived as a 'digital right' or traditionally considered part of the digital rights movement's agenda - despite this being a key feature of the movement at a global level and more recently within the EU as well as representing a crucial thread in the fabric for advancing digital rights.

OPPORTUNITIES

There are a number of opportunities for the UK and EU to advance digital rights protections at a national, regional and global level set out sequentially below:

UK opportunities for advancing digital rights in 2025

As set out by the Minister for the Department of Science, Innovation and Technology, Peter Kyle, to the House of Commons: "The future of technology is ours to shape, and the opportunities it offers are ours to seize."[5] At the close of 2024, the UK government envisioned "a future where technology enriches the life of every single citizen" and that also offers "unequivocal" support for human rights.[6] The AI Opportunities Action Plan also emphasises "the importance of fostering public trust in technology, particularly considering the interests of marginalised groups."[7]

5 Peter Kyle (2024) "Technology in Public Services. Volume 753: debated on Monday 2 September 2024." UK Parliament. https://hansard.parliament.uk/commons/2024-09-02/debates/721F0511-796C-49C4-A4FF-E0528E6419C6/TechnologyInPublicServices
6 Ibid; Attorney General's Office (2024) Attorney General's Bingham Lecture on the rule of law https://www.gov.uk/government/speeches/attorney-generals-2024-bingham-lecture-on-the-rule-of-law;
7 DSIT (2025) "AI Opportunities Action Plan." https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

We recommend that the UK government facilitates this vision by developing and adopting a UK Declaration of Digital Rights & Principles. Such a declaration would not be legally binding in order to avoid adding additional complexity and incoherence to existing regulation. Instead, it would act as a set of foundational and organising rights and principles with which to both cohere, explain and identify gaps in existing policies and legislation, as well as to inform and motivate new policies and legislation relating to technology that could strengthen public trust.

Through the development of such a Declaration, if conducted via a deliberative process supported by policymakers and informed by the expertise of digital rights experts and technologists, we can better understand and reflect the needs, values and priorities of citizens and, as a result, enable citizens to truly understand, shape and trust in the future of technology.

We see six benefits for developing and declaring a set of Digital Rights and Principles, if following a process set-out below:

1. **Strengthened citizen trust in technology** - particularly crucial when such technology is deployed as part of a public service reform agenda
2. **Citizen empowerment** - providing an opportunity to refine and clarify the language of digital rights with citizens enabling them to better protect themselves online, behave responsibly, understand what existing legal protections are available to them and seek remedy if their rights are abused - and to hold policymakers accountable.
3. **Technological innovation** - providing clearer goalposts and guardrails for industry
4. **Policy and regulatory coherence** - enabling policymakers across the UK government to align, communicate and evaluate policy and legislation against a consistent framework
5. **Stronger civil society collaboration and alignment** - enabling digital rights advocates the space to clarify, align, unite and consolidate behind a shared platform of advocacy on what is an uneven playing field relative to the technology industry lobby
6. **Regional and global partnerships** - providing the instruments to build regional and global partnerships to facilitate rights protections for all, regardless of citizenship status.

In 2025, we will contine to see waves of new digital policy and legislation in the UK – clarifying the foundations for citizens' digital rights which need protecting and enabling in a holistic framework to inform a Declaration of Digital Rights & Principles is therefore an urgent task to support and guide this work. The following recommendations present a path to its adoption, with additional intermediary benefits in the process of its development.

1.1 Establish a UK digital rights network to include social, racial and economic justice organisations: Convene as a network to meet, share knowledge, align on priorities across the breadth and diversity of digital rights and shared goals.

1.2 Clarify digital rights language: Drawing on the digital rights network (1.1) as an advisory and guiding body, funders should invest in qualitative research with the public, particularly with different marginalised communities, to explore and clarify the language that could be used to discuss and define digital rights.

1.3 Develop a UK digital rights framework through a deliberative process: The UK government and/or other funders should invest in a deliberative process with the public to identify and refine the priorities for a cohesive digital rights framework, much like the EU's Declaration of Digital Rights and Principles and South Korea's Digital Bill of Rights.

1.4 Digital rights coalition to coordinate a united communications campaign: The new digital rights coalition could develop a united strategic communications campaign that highlights why

digital rights protections do not limit or undermine innovation and growth.

1.5 UK policymakers should adopt a citizen-led Declaration of Digital Rights and Principles: This adoption could be borne out of initial support and involvement in the deliberative process, either/ both as a funder and an influencer in the design and parameters of the discussion. DSIT could then use such a Declaration to: evaluate existing policy approaches; invite colleagues in other departments to highlight potential new policy approaches for strengthening digital rights protections; and share annual progress reports towards digital rights protections goals over the course of this and the next Parliament.

Regional opportunities for advancing digital rights in 2025

Whilst the following opportunities could largely apply to any regional bodies, these opportunities are written specifically for European policymakers.

2.1 Explore how the new EU 'Digital Rights and Principles' could be incorporated into existing European rights legislation.

2.2 Strengthen digital collaboration by expanding regional partnerships to co-create inclusive, secure, and sustainable digital infrastructures and governance frameworks.

2.3 Enhance advocacy through coordinated funding mechanisms to support smaller digital rights organisations with limited resources and the lobbying power of large tech companies.

Global opportunities for advancing digital rights in 2025

3.1 The UN could establish and coordinate a Global Fund for Digital Infrastructure as proposed by the Global Digital Compact.

3.2 UNESCO, working with regional bodies, could implement AI readiness assessments within participating regions, building on its existing Readiness Assessment Methodology.

3.3 The UN could establish a global framework that standardises data access for research and platform oversight.

3.4 International organisations, particularly the UN and ITU, could design digital access initiatives that explicitly address structural power imbalances in connectivity and infrastructure.

1. INTRODUCTION

Now that the United Nations commits to a Global Digital Compact, the rights-based governance model of digital technologies is gaining momentum.[8,9] Chasing the tail of rapid technological innovation, a drumbeat of legislation from the European Union (EU) has cemented what some refer to as the EU's rights-driven regulatory model.[10] Historically, such a model has proven globally influential via 'the Brussels Effect' - where, for example, the EU's General Data Protection Regulation became the global data privacy standard for global tech companies and countries from Japan to Brazil.[11] In sharp contrast to the US' market-driven governance model which has focused on incentivising innovation and prioritising free speech, the EU model seeks to balance citizens' rights relative to both technology companies and the state.[12]

Whilst strongly divergent priorities have emerged between China, the USA and Europe, globally we are observing an evolution of human rights norms and discourse surrounding 'digital rights'. As symbolised by the European Declaration on Digital Rights and Principles (2022) and South Korea's Digital Bill of Rights (2022), new digital rights now influence considerations for how we protect and enable the basic needs of global citizens in a digital world.[13] The universality of human rights and application to all equally - irrespective of one's nation - requires global cooperation and indeed the EU is not alone in advancing a rights-based model of governance.[14] This growing global movement is particularly visible in the Global South, where regional bodies like the African Union are developing frameworks that ensure human rights protections with the emergence of technologies.[15]

In this paper, we at Demos explore the challenges, trends, approaches taken and opportunities for advancing digital rights in the UK and the EU. The Oxford Martin School's AI Governance Initiative has also contributed reflections on trends and opportunities at a global, multilateral level.[16]

As a UK-based think tank, we at Demos have reflected on the UK's own model of technological governance - balanced between the influences of the US and the EU as well as China's state-

8 United Nations (2024) Global Digital Compact. https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf
9 Denardis, L. (2020) "The Internet in Everything: Freedom and Security in a World with No Off Switch". Yale University Press https://doi.org/10.2307/j.ctvt1sgc0.
10 Lehdonvirta (2022) Cloud Empires; Bradford, 2023, Digital Empires.
11 Bradford (2023) Digital Empires: The Global Battle to Regulate Technology
12 Ibid
13 European Declaration on Digital Rights and Principles (2022) https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles
14 Universal Declaration of Human Rights, Amnesty International. https://www.amnesty.org/en/what-we-do/universal-declaration-of-human-rights/#:~:text=The%2030%20rights%20and%20freedoms,to%20life%2C%20liberty%20and%20privacy
15 African Commission on Human and Peoples' Rights. (2024) 'Resolution on the Need to Undertake a Study on Human and Peoples' Rights and Artificial Intelligence (AI), Robotics and Other New and Emerging Technologies in Africa - ACHPR/Res. 473 (EXT.OS/ XXXI) 2021' https://achpr.au.int/en/adopted-resolutions/473-resolution-need-undertake-study-human-and-peoples-rights-and-art; African Commission on Human and Peoples' Rights. (2024) ACHPR Focal Point on the Study on Human and Peoples' Rights and AI, Robotics and Other New Technologies Convening Consultation Meeting on the Study in Kigali, Rwanda https://achpr.au.int/en/news/press-releases/2024-09-30/ai-robotics-new-technologies-consultation-meeting-study-kigali.
16 Ministry of Science and ICT, Republic of Korea (2022). https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&bbsSeqNo=42&nttSeqNo=801

driven model - at a pivotal moment. In 2025, eight years after the UK voted to exit the European Union, grappled with repealing the Human Rights Act and weakening ties to the European Court of Human Rights (ECHR), a recent change of government has borne a new era of European relations and "unequivocal" support for human rights and the European Convention on Human Rights.[17]

While the UK currently lacks a broader digital rights framework or bill, a new wave of legislation – from the Data Use and Access Bill, Fraud, Debt and Error Bill and the Artificial Intelligence Bill, to policies such as the AI Opportunities Plan and a new digital inclusion strategy – presents a refreshed opportunity to explore how the UK can strengthen digital rights protections.

In this context, we investigate:

- What we mean by 'digital human rights' and the opportunities and challenges different framings present to advancing global human rights protections
- Recent common-ground trends and challenges in the protection of digital rights faced by those advancing such protections in the UK and EU
- Examples of the policy-based and legal approaches to the protection of digital rights in the UK and EU and how these relate to approaches taken in South Korea and at a global, multilateral level
- Opportunities and key reflection questions for policymakers and human rights activists in the advancement of digital rights

This paper was developed between August and December 2024 based on a literature review on the digital rights movement, analysis of a sample of policies and legislation from the UK, EU, and global trends, 20 expert interviews, a roundtable with UK and EU digital rights organisations and academics conducted in October 2024 and workshops with UK and EU digital rights organisations, policymakers and academics in December 2024. The paper was paused for publication until February 2025 while Demos gathered co-signatories for an open letter to support its publication.

17 Ministry of Justice, UK Government (2022) Bill of Rights to strengthen freedom of speech and curb bogus human rights claims https://www.gov.uk/government/news/bill-of-rights-to-strengthen-freedom-of-speech-and-curb-bogus-human-rights-claims; Attorney General's Office (2024) Attorney General's Bingham Lecture on the rule of law https://www.gov.uk/government/speeches/attorney-generals-2024-bingham-lecture-on-the-rule-of-law; European Commission (2024) Statement by the President of the European Commission and the Prime Minister of the United Kingdom on Enhancing Strategic Cooperation, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_24_5003

2. BACKGROUND

2.1 DEFINING DIGITAL RIGHTS

Generally speaking, the goal of 'digital rights', as with all human rights, is to protect and enable the basic rights and freedom that all people are entitled to - but applied to the digital world.

Yet, the definition of 'digital rights' is unsettled. Its meaning has been conceived from a smorgasbord of legal frameworks ranging from fundamental human rights declarations to data protection, cybersecurity, consumer rights and copyright legislation - evolving in the hands of different digital rights movements submerged in different political, social and legal contexts.[18]

Here we divide digital rights into two broad categories and provide examples in Figure 1:

2.1.1 Digital rights as an extension of human rights into the digital world

Some regard and defend digital rights as a natural extension of human rights into a digital sphere characterising these as a 'reinterpretation of existing rights'.[19]

This relationship between digital rights and their existing fundamental roots is crucial to those who seek to strengthen the international legitimacy and credibility of digital rights when advocating for consistent regulation of global platforms. For this reason, some organisations such as the Alliance For Universal Digital Rights, are calling for the adoption of 'Digital Principles' "rooted in human rights law".[20] Others, such as the Digital Freedom Fund, have invested in campaigns that highlight the interconnection between human and digital rights.[21]

Human rights abuses in the digital sphere can sometimes feel opaque or invisible to an individual, such as the leak of personal data or the bias of an algorithm towards a marginalised group. Therefore, by articulating how a human right, such as the right to privacy or the right to non-discrimination, extends into the digital sphere, it becomes possible to explain how what has occurred online translates into being an abuse of fundamental human rights.

2.1.2 Digital rights as distinct and wholly new rights

In addition to extensions of pre-existing 'offline' human rights into the digital sphere, there are also wholly new digital rights emerging that have no equivalent in the offline world. For example, the right to digital access, the right to disconnect and the right to participate in technological development.[22] Both the European Declaration on Digital Rights and Principles

18 Warso (2023) Digital Rights Revisited https://openfuture.eu/wp-content/uploads/2023/10/231017Digital-rights-revisited.pdf; Postigo (2012) "The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright", The Information Society Series 7

19 Dror-Shpoliansky and Shany (2021) "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology", European Journal of International Law 32 (4): 1249–1282;

20 Alliance for Universal Digital Rights. (2024) Digital Principles. https://audri.org/our-digital-principles/

21 Digital Freedom Fund (2020) Digital rights are human rights https://digitalfreedomfund.org/wp-content/uploads/2020/12/Human-Rights_V3.pdf

22 Pollicino (2019) "Right to Internet Access: Quid Iuris?" In: von Arnauld, von der Decken, Susi (eds), The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric, Cambridge University Press

and the South Korean Digital Bill of Rights explicitly establish the right to digital access - with South Korea guaranteeing a 'stable network environment and to access and use various digital services anywhere and anytime without discrimination' and the EU ensuring 'access to affordable and high-speed digital connectivity.' In the French government's Digital Republic Bill we see provision for 'universal access to digital technology'.[23] Both the EU and South Korean frameworks also introduce new environmental rights specific to the digital age, requiring the minimization of technology's environmental impact and promoting sustainable digital product life cycles.

Such inventions reflect what some argue are a failure of traditional human rights frameworks to protect human rights in a digital ecosystem that is fundamentally different to the offline world.[24]

Together, these two pathways - the extension of existing human rights into the digital world and the introduction of wholly new digital rights - demonstrate how new rights, norms and principles are being developed to address gaps in traditional frameworks and provide protections specifically needed in the digital world.

23 Republique Francais, Digital Republic Bill. https://www.republique-numerique.fr/pages/digital-republic-bill-rationale; Custers (2022) "New digital rights: Imagining additional fundamental rights for the digital era" Computer Law & Security Review, Volume 44

24 Cocito and De Hert (2023) "The transformative nature of the EU Declaration on Digital Rights and Principles: Replacing the old paradigm (normative equivalency of rights)" Computer Law & Security Review 50.

FIGURE 1
'DIGITAL RIGHTS' FRAMEWORKS AND RIGHTS EXAMPLES

Please note the following examples of digital rights are not exhaustive, but are indicative of how new digital rights are evolving and are represented in indicative instruments relative to more fundamental human rights instruments of the Universal Declaration of Human Rights (UDHR) and the European Convention of Human Rights (ECHR).

	UDHR[25]	ECHR[26]	South Korean Digital Bill of Rights[27]	European Declaration on Digital Rights[28]
1. Digital rights that are a reinterpretation of preexisting human rights				
Freedom of expression	**Article 10:** Freedom of expression	**Article 10:** Freedom of expression	**Article 7:** Freedom of Digital Expression: Every individual shall be able to freely express their views in the digital environment; provided, however, that such expression shall be carried out responsibly so as not to infringe upon the honor and rights of others, public morality, or social ethics	**Article 13:** Everyone has the right to freedom of expression and information, as well as freedom of assembly and of association in the digital environment. **Article 15:** Online platforms, particularly very large online platforms, should support free democratic debate online. Given the role of their services in shaping public opinion and discourse, very large online platforms should mitigate the risks stemming from the functioning and use of their services, including in relation to misinformation and disinformation campaigns, and protect freedom of expression

25 Amnesty International UK. Universal Declaration of Human Rights. https://www.amnesty.org/en/what-we-do/universal-declaration-of-human-rights/#:~:text=The%2030%20rights%20and%20freedoms,to%20life%2C%20liberty%20and%20privacy.
26 Council of Europe, European Court of Human Rights. European Convention of Human Rights. https://www.echr.coe.int/documents/d/echr/convention_ENG
27 South Korean Digital Bill of Rights. (2023) https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=
28 European Declaration on Digital Rights and Principles (2022) https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

The right to education	**Article 26:** Everyone has the right to education.	**Protocol Article 2:** Right to education	**Article 14:** The digital divide shall be bridged to ensure opportunities for the development and use of digital technology, and educational opportunities shall be provided for the improvement of digital literacy.	**Article 4:** Everyone has the right to education, training and lifelong learning and should be able to acquire all basic and advanced digital skills.
Non-discrimination	**Article 2:** Everyone is equal regardless of race, colour, sex, language, religion, politics, or where they were born.	**Article 14:** Prohibition of discrimination	**Article 12:** Everyone should have access to a trustworthy, diverse and multilingual digital environment. Access to diverse content contributes to a pluralistic public debate and effective participation in democracy in a non-discriminatory manner.	**Article 8:** Every individual shall be protected from unjust discrimination and bias arising from digital technology and shall be respected for their social and cultural diversity
Privacy	**Article 12:** Everyone has the right to privacy and freedom from attacks on their reputation.	**Article 8:** Right to respect for private and family life	**Article 19:** In the digital environment, the privacy of individuals shall be protected from unlawful identification and tracking, including digital surveillance and location tracking.	**Article 17:** Everyone has the right to privacy and to the protection of their personal data. The latter right includes the control by individuals on how their personal data are used and with whom they are shared. **Article 18:** Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and not to be subjected to unlawful online surveillance, unlawful pervasive tracking or interception measures.

2. Digital rights that are distinct and wholly new rights			
Digital access	*No comparable pre-existing human right*	**Article 6:** Every individual shall be guaranteed a stable network environment and to access and use various digital services anywhere and anytime without discrimination through the same	**Article 3:** Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity.
Environmental protection	*No comparable pre-existing human right*	**Article 26:** Nations shall endeavour to collaborate with the international community to minimize the negative impacts and harm of digital technology on the environment, ecology, and the climate system, while also contributing to enhancing the well-being of the global community through the utilization of digital technology.	**Article 23:** To avoid significant harm to the environment and to promote a circular economy, digital products and services should be designed, produced, used, repaired, recycled and disposed of in a way that mitigates their negative impact on the environment and on society and avoids premature obsolescence

2.2 POTENTIAL SHORTCOMINGS OF CURRENT DIGITAL RIGHTS DEFINITIONS

Whilst human rights advocates have emphasised the importance of digital rights - whether they are explicit extensions or wholly new - there is a strong awareness of the potential risks implicit to their development.

2.2.1 Alienation of social justice movements

By creating new articulations of human rights in the digital sphere and creating wholly new digital rights, there is a risk that traditional social justice movements or human rights activists feel disempowered or less able to contribute their expertise to digital policymaking because of concerns about a lack of understanding of the digital world. This has been a key concern for digital rights activists since responses to the Snowdon scandal were perceived as predominantly weighted towards techno-legal solutions relating to the development and use of encryption and policy advocacy around privacy and data protection, and didn't sufficiently engage with impacted communities.[29] For this reason, in discussions about how we define digital rights and their implications for policy, digital rights advocates have emphasised the importance of engaging the public and wider social justice movements, and foregrounding the voices of those affected by online harms.

2.2.2 Encouraging tech-centred or short-term solutions

Articulating both explicit extensions of human rights into the digital sphere and wholly new digital rights can also risk encouraging techno-centred solutions, rather than recognising the wider social or cultural contexts or factors which also enable harms in the digital world or by digital technologies. For example, there are risks of discriminatory outcomes when facial recognition technology is used by law enforcement both because of the biases laden within the technology *and* because of the harmful cultural and psychological biases of the institutions and individuals that deploy them. Thus, the clarity of defining digital rights is important for shedding light on the specific harms intrinsic to the technology, but it remains important not to lose sight of the overall socio-cultural ecosystems e.g. of discrimination that contribute to and exacerbate them.[30]

Original fundamental human rights, as articulated in the Universal Declaration of Human Rights (UDHR), such as 'the right to privacy' or 'the right to freedom of expression', have been both celebrated and critiqued for their longevity irrespective of the evolving context in which they are enacted. For this reason, new digital rights articulations developed from these original frameworks risk becoming quickly dated as specific forms of technology emerge or fade into obsolescence. This is another reason why human rights advocates emphasise the importance of continuously linking digital rights back to their fundamental antecedents, to enable consideration of how they must evolve and take on new meaning as our digital contexts reform.

29 Jansen et al (2023) The Climate Crisis is a Digital Rights Crisis: Exploring the Civil-Society Framing of Two Intersecting Disasters. In LIMITS '23: Workshop on Computing within Limits, June 14–15, 2023. https://doi.org/10.21428/bf6fb269.b4704652; Dencik, Hintz, and Cable. (2016). "Towards data justice? The ambiguity of anti-surveillance resistance in political activism." Big Data & Society 3, 2 (2016), 1–11. https://doi.org/10.1177/2053951716679678

30 Pena Gandadharan and Niklas (2019) "Decentering technology in discourse on discrimination." Information, Communication and Society, 22:7, 882-899.

3. DIGITAL RIGHTS TRENDS

Over the last twenty five years, the digital rights movements in Europe, and more recently in the UK, have evolved and deepened as new digital harms have emerged.

UK and EU-based digital rights advocates have had frustrations that policymakers are slow to legislate and protect citizens until there is sufficient public outcry following a scandal. The resulting responsive lockstep cycle has been described as 'regulation by headline'. However, in recent years, two new trends are providing hope for a break in this cycle: the emergence of holistic digital rights frameworks and widening considerations of wholly new digital rights such as access, skills and inclusion in technological development. With these two new trends, the diversity of the digital rights movement has multiplied and with it, the opportunity for more preventative policymaking.

This section provides a high-level overview of six **waves of digital rights governance, legislation and policy development at the EU and UK** level. We also reference significant global digital rights trends shaping the UK and EU agenda. Please note that many of the waves described overlap in time:

3.1 FOUNDATIONAL WAVE

In the 1990s, the seeds of digital rights were sown with the formation of a number of key global internet governance fora, such as the World Summit on the Information Society (WSIS). The long-standing International Telecommunication Union (ITU) also adopted the Declaration on Freedom of Expression formalising online freedom of expression within UN frameworks and promoting broadband access to reduce the digital divide.

3.2 PRIVACY WAVE

The late 1990s and early 2000s saw the launch and rapid growth of the world's tech giants, from Google to Facebook. It was at this time and against this backdrop of rapidly evolving digital worlds that the cornerstones of the digital rights movement in Europe, the European Digital

Rights Initiative network (EDRi), was founded. In the UK too, a Labour government sought to establish the use of digital identity cards, via the Identity Cards Act in 2006 - a move that was contested by privacy advocates and later repealed by a Conservative government. This period was thus dominated by privacy rights and anti-surveillance advocates highlighting the needs for stronger data protection and encryption.

The privacy rights narrative came into full bloom when fueled by a global scandal.[31] Between 2014 and 2015, after Edward Snowdon blew the whistle on state surveillance, the movement gained new momentum and achieved what is now seen as one of the most influential forms of technology regulation: the EU's General Data Protection Regulation (GDPR).[32] The GDPR has been widely regarded as a turning point in the relationship between the state and technology companies, particularly symbolised by the Facebook vs Data Protection Commissioner case in 2015. However, the ability to enforce such legislation has remained a challenge for states and represented an ongoing frustration for the digital rights movement as new legislation emerges.[33] See 'Appendix: Case Study 1' for more detailed evaluation of the GDPR and concerns surrounding enforcement and remedy.

Globally, this emphasis on censorship and surveillance was echoed throughout the 2010s. Over 350 resolutions by the UN General Assembly (UNGA) and the Human Rights Council (HRC) reflected such issues. For example, reports by Special Rapporteurs Frank Le Rue and David Kaye provided critical analyses of digital privacy and surveillance, advocating for robust safeguards in the digital age.[34,35]

Digital access also continued to receive focus at a global level with the establishment of the High-Level Panel on Digital Cooperation in 2011 and the integration of digital technologies into the Sustainable Development Goals (SDGs) in 2015.

3.3 DIVERSIFICATION OF DIGITAL RIGHTS WAVE

By 2018, social media platforms had gained new global reach and with it allegations of a much broader range of technologically-enabled harms to both democracy and human life. A United Nations report on the "determining role" of Facebook in the Myanmar genocide highlighted the risks of limited content moderation and engagement-based algorithms in the spread of violent content and threats to marginalised communities.[36] In the UK, the suicide of Molly Russell, a teenager engaging in suicide-related content online, also raised outcries regarding children's rights and safety.[37] The revelations regarding the role of Cambridge Analytica and Facebook in the 2016 US election and Brexit referendum also highlighted concerns regarding the power of platforms to influence voters and with them, democratic elections.[38] Such a series of significant evidence of harm built public and policy-level support for stronger regulation in the EU and UK.

31 Perception of a privacy, anti-surveillance and data protection focus was repeated persistently throughout expert interviews with European and UK human rights advocates in September 2024; Also Jansen et al (2023). The Climate Crisis is a Digital Rights Crisis: Exploring the Civil-Society Framing of Two Intersecting Disasters. In LIMITS '23: Workshop on Computing within Limits, June 14–15, 2023. https://doi.org/10.21428/bf6fb269.b4704652

32 Greenwald, MacAskill and Poitras (2013) Edward Snowden: the whistleblower behind the NSA surveillance revelations. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; European Digital Rights Network (2024) Victories https://edri.org/about-us/victories/

33 Global Freedom of Expression, Columbia University (2024) Data Protection Commissioner v. Facebook (Schrems II). https://globalfreedomofexpression.columbia.edu/cases/data-protection-commissioner-v-facebook-schrems-ii.

34 Kaye (2019) "Report to the Human Rights Council on the surveillance industry and human rights implications" UN Special Rapporteur on freedom of opinion and expression.https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance.

35 La Rue(2013) "Report to the Human Rights Council on privacy and freedom of expression as interlinked and mutually dependent rights in the digital age" UN Human Rights Council.https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age.

36 BBC (2018) https://www.bbc.co.uk/news/technology-43385677

37 Milmo (2022) "'The bleakest of worlds': how Molly Russell fell into a vortex of despair on social media." https://www.theguardian.com/technology/2022/sep/30/how-molly-russell-fell-into-a-vortex-of-despair-on-social-media

38 The Guardian (2018) Cambridge Analytica Files. https://www.theguardian.com/news/series/cambridge-analytica-files

By 2024, after significant negotiation across civil society and the tech industry, both the European Union and the UK had advanced a range of legislation to protect user safety online reflecting a range of digital rights (in the form of the Digital Services Act (2022) and Online Safety Act (2023).[39] Yet, while some have praised both the Digital Services Act and, to a lesser extent, the Online Safety Act for their progress in protections in specific areas, rights advocates have remained dissatisfied with what has been prioritised within such legislation and the trade-offs between different areas of human rights. See 'Appendix: Case Study 2' for more detailed evaluation of these policy areas and a discussion below of the challenges of balancing different human rights protections in the UK specifically.

3.4 PREVENTATIVE WAVE

A more recent trend in the EU and the UK that has been viewed positively by rights advocates is a range of legislation that seeks to moderate and balance the power and influence of the technology companies themselves relative to other industries. For example, the EU's Digital Markets Act (2022) and the UK's Digital Markets, Competition and Consumers Act (2024) have both been praised as offering a key lever for tackling the outsized power of technology companies that undermines the ability to negotiate and protect citizens.[40] The European Union has also successfully advanced its AI Act while the UK has begun work on its own Frontier AI Bill demonstrating a focus on regulating specific technologies (see Appendix: Case Study 3). Though, as highlighted below (see Section 4. Challenges), concerns remain about whether such legislation can balance the perceived trade-offs between economic growth, security and rights protections.

3.5 DECOLONISING WAVE

In recent years, digital rights movements in Europe, particularly led by EDRi and the Digital Freedom Fund, have moved to decolonise the digital rights movement with an emphasis on ensuring the concerns of marginalised communities are reflected in their advocacy work. This has included, for example, consideration of the role of digital rights in migration and climate justice.[41] Key to this project is a stronger emphasis on the inclusion of social, racial and economic justice organisations in the development of the movement's priorities, starting with understanding the digital rights issues affecting their communities. This has resulted in a stronger consideration of the specific and disproportionate harms that are caused by technologies on marginalised groups, including policies by police and immigration control, as well a focus on access to an affordability of digital devices and connectivity.[42] The decolonization wave has seen increased calls for the distribution of global digital governance beyond the influence of a handful of large developed nations.[43] It is with this reformed approach that we see a stronger connection solidifying with the long-standing focus of global digital rights priorities - that of tackling the digital divide in the form of digital access, skills, and governance.

39 European Commission (2022) Digital Services Act https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en; DSIT (2023) Online Safety Act Explainer. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

40 European Commission (2022) Digital Market's Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en; UK Parliament (2024) Digital Markets, Competition and Consumers Act, https://bills.parliament.uk/bills/3453

41 EDRi (2024) "Decolonising Digital Rights." https://edri.org/what-we-do/decolonising-digital-rights/

42 Digital Freedom Fund and EDRi (2021) "Creating conditions for a decolonised digital rights field". https://edri.org/our-work/creating-conditions-for-a-decoloniseddigital-rights-field/

43 United Nations (2024) Global Digital Compact. https://www.un.org/global-digital-compact/en

3.6 DEMOCRATISATION WAVE

3.6.1. An evolution in global norms

As highlighted in Section 3, new digital rights are emerging both via new national instruments such as the South Korean Digital Bill of Rights, but also at a global level through the growing acknowledgment of new norms and principles specific to new digital technologies. This is exemplified by UNESCO's Recommendation on the Ethics of AI which introduces entirely new proposals for requirements of AI systems to be transparent and accountable in ways that traditional rights frameworks never contemplated.[44] UNESCO's AI Readiness Assessment framework also creates unprecedented standards for algorithmic fairness and inclusion, prioritising the elimination of bias in AI applications and ensuring non-discriminatory participation in AI policy-making.[45] Similarly, the new Global Digital Compact advances novel principles around "human oversight of technology" and facilitates a global effort drawing contributions from thousands of individuals worldwide to make digital spaces safe, secure, and accessible to all.[46] These global instruments collectively assist in normalising new rights - from algorithmic accountability to equitable access to AI resources.

3.6.2 Transformation in conceptions of digital access

Conceptualisations of digital access as a right specifically, at a global level, have undergone a profound transformation. Digital access rights have evolved from a focus on basic internet connectivity in the early 1990s to a more comprehensive understanding encompassing both access to and participation in technological development.[47,48] This trend reflects recognition that 'technological dependency' undermines other human rights, such as limiting access to information, freedom of expression or access to educational opportunities and work.[49] For instance, limited access to digital platforms can restrict freedom of expression and access to information and lack of digital access can impair educational opportunities as resources move online.[50,51] The evolution in this conception has spurred new international frameworks like UNESCO's Global Framework of Digital Literacy Skills and advanced digital skills for participation in the digital economy. This progression has emphasised that meaningful access to and participation in the digital world requires not only basic and critical digital literacy, but also an understanding of digital rights and responsibilities.[52,53]

Given this transformation in the conceptualisation of digital access and skills at a global level, as represented within the EU's Digital Rights and Principles and South Korea's Digital Bill of Rights, it remains to be seen whether the UK's digital access and skills policies can also evolve in line with the rights agenda. (See Appendix: Case Study 4 and 5 for an overview of the current policies).

44 UNESCO (2021) Recommendation on the Ethics of Artificial Intelligence. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
45 UNESCO (2023) Readiness assessment methodology: a tool of the Recommendation on the Ethics of Artificial Intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000385198
46 United Nations (2024) Global Digital Compact. https://www.un.org/global-digital-compact/en
47 Karppinen and Puukko. (2020) 'Four Discourses of Digital Rights: Promises and Problems of Rights-Based Politics'. Journal of Information Policy 10: 304–28. https://doi.org/10.5325/jinfopoli.10.2020.0304.
48 OECD. (2024) 'Shaping a Rights-Oriented Digital Transformation' https://www.oecd.org/en/publications/shaping-a-rights-oriented-digital-transformation_86ee84e2-en.html.
49 UN Conference on Trade and Development (2023) Digital Economy Report
50 Schippers (2018) "Why technology puts human rights at risk." The Conversation. https://theconversation.com/why-technology-puts-human-rights-at-risk-92087
51 Baweja and Singh (2020) "Beginning of Artificial Intelligence, End of Human Rights". LSE Blog. https://blogs.lse.ac.uk/humanrights/2020/07/16/beginning-of-artificial-intelligence-end-of-human-rights/
52 UNESCO (2018) "A global framework of reference on digital literacy skills for indicator 4.4.2"https://unesdoc.unesco.org/ark:/48223/pf0000265403
53 Law, Woo & Wong (2018) "A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2. UNESCO Information " Paper No. 51 https://docs.edtechhub.org/lib/QB69UIDS

4. DIGITAL RIGHTS CHALLENGES IN THE UK AND EU

UK and EU rights advocates highlighted a number of pre-existing challenges with advancing digital rights, some of which interconnect with challenges at a global level. Of course, the European and UK contexts are very different, particularly with regards to socio-cultural norms surrounding human rights. This is symbolised by the fact that the EU has already launched a Declaration of Digital Rights and Principles, while the UK lacks one. This chapter commences by setting out the common themes (4.1- 4.5), before focusing specifically on challenges unique to the UK context (4.6-4.7).

4.1 IT'S "AN UNEVEN PLAYING FIELD"[54]

4.1.1 Global power in the balance

A prominent challenge emphasised repeatedly by digital rights activists both in the EU and UK is an imbalance of regulatory power that mirrors the global digital divide. Such a divide is exemplified by inequities in technological development and participation. For example:

- 75% of AI research capacity is concentrated in North America, Europe, and China
- Less than 2% of major AI conference papers come from Africa
- Technological development often fails to address the needs of marginalized communities
- Language barriers exclude many communities from technological participation.[55]

54 Quotation from an anonymised interview with digital rights organisation
55 Oxford Martin School. (2024) 'Voice and Access in AI: Global AI Majority Participation In…'. https://www.oxfordmartin.ox.ac.uk/publications/voice-and-access-in-ai-global-ai-majority-participation-in-artificial-intelligence-development-and-governance.

Some of the most prominent examples of online harms emanate from some of the most resource-poor countries and where regulations that protect digital rights are lacking. For example, less than 35% of the populations in Myanmar and Ethiopia have access to the internet.[56] In such countries, the internet is more likely to be shut down by the government than regulated.[57] Furthermore, Facebook algorithms are said to have exacerbated violence against minority communities in both countries, namely the Rohingya in Myanmar and the Tigrayan community.[58] For a range of multi-faceted reasons including a lack of resources, such countries are much less likely to develop legislation that protects the rights of their citizens in the face of technological advancement. This global imbalance underpins why many digital rights advocates in the UK and EU and around the globe emphasise the need for the participation of the global community to strengthen global digital rights frameworks, norms and principles and coordination to help prevent such harms in countries with weaker pre-existing protections.

4.1.2 Corporate interests relative to the citizen

Despite Europe being a comparatively resource-rich region with high levels of internet penetration and itself advancing the rights-model, there also remains power imbalances within the negotiations of key governance instruments - namely between digital rights organisations, state authorities and tech companies. For example, during the 'Preventative wave' described above and the formulation of regulation such as the EU's Digital Services Act and Digital Markets Act, Apple, Google, and Meta spent €6.5 million, Microsoft €6 million, and Amazon €7 million on lobbying efforts in the EU in order to advance their needs and, in some cases, weaken digital rights protections.[59] In the same year, 75% of the meetings held with the European Commission were with corporate bodies, relative to 19% from NGOs.[60] Such well resourced lobbying stands in contrast to the small policy teams of digital rights organisations whose time and expertise is also spread across an escalating number of policy areas and bills as technology becomes interwoven into more and more contexts.[61] This imbalance places a heavier weight on digital rights organisations who "are burned out and just under-resourced."[62]

Digital rights activists in the EU highlighted frustrations with an imbalance towards corporate interests, that may be entrenched in other socio-legal cultures, during discussions regarding new EU legislation. For example, during the Digital Services Act negotiations, if an American corporate has an understanding of freedom of expression as an absolute right relative to a European who recognises freedom of expression as a qualified right i.e. where the state can lawfully interfere under certain circumstances. Another more recent example of these tensions during negotiations includes surrounding the EU's Ad Hoc Committee on Artificial Intelligence (CAHAI) and later the Council of Europe's Committee on Artificial Intelligence, digital rights activists described the non-stop struggle to protect fundamental rights when

56 Statista (2024) "Internet penetration rate in Myanmar from 2011 to 2020". https://www.statista.com/statistics/766034/internet-penetration-rate-myanmar/#:~:text=In%202020%2C%20approximately%2035.1%20percent,Myanmar%20were%20using%20the%20internet.; Center for the Advancement of Rights and Democracy (2024) Digital Divide. https://www.cardeth.org/digital-divide#:~:text=Only%2024%25%20of%20Ethiopians%20have%20access%20to%20the%20internet&text=In%20Ethiopia%2C%2024%25%20of%20people,people%20have%20no%20internet%20access.&text=And%20there%20is%20data%20to%20back%20up%20these%20claims.

57 Access Now (2023) "Preserving freedom in crisis: Ethiopia's internet shutdowns must not become the norm". https://www.accessnow.org/press-release/open-statement-internet-shutdown-amhara/ ; Access Now (2024) "Myanmar's iron curtain: internet shutdowns and repression in 2023".https://www.accessnow.org/press-release/myanmar-keepiton-internet-shutdowns-2023-en/ https://www.accessnow.org/press-release/myanmar-keepiton-internet-shutdowns-2023-en/

58 Amnesty International (2023) "A Death Sentence For My Father" Meta's Contribution To Human Rights Abuses In Northern Ethiopia. https://www.amnesty.org.uk/files/2023-10/Amnesty%20International%20Tigray%20Meta%20Report.pdf?VersionId=TcqfAYDhZAX2MhsXMj7acym5gc6GMTQG, Amnesty International (2023) "The Social Atrocity Meta And The Right To Remedy For The Rohingya" https://www.amnesty.org/en/documents/asa16/5933/2022/en/

59 Lombardi (2022) "Big Tech boosts lobbying spending in Brussels". https://www-politico-eu.ezproxy-prd.bodleian.ox.ac.uk/article/big-tech-boosts-lobbying-spending-in-brussels/

60 Corporate Europe Observatory and Lobby Control e.V](2021) "The Lobby Network: Big Tech's web of influence in the EU". https://corporateeurope.org/sites/default/files/2021-08/The%20lobby%20network%20-%20Big%20Tech%27s%20web%20of%20influence%20in%20the%20EU.pdf.

61 Zuboff, S (2019) "The Age of Surveillance Capitalism". Profile Books.

62 Quotation from anonymised interview provided by a representative of a digital rights organisation

even representatives of states advocated for 'green lines' in "cases where you have to deploy AI" citing the benefits to growth.[63] A final example in the EU AI Act negotiations was the resistance by private sector actors to impact assessment requirements for their AI systems. These requirements were ultimately removed and retained only for public sector systems. The level of advocacy required by digital rights activists was felt to be repeatedly outstripped and undermined by the significant influence of the tech lobby whose emphasis on the relative benefits of innovation and growth to the region was felt to have powerful influence over the negotiations.

To tackle this imbalance between corporate interests and civil society organisations' recommendations, digital rights advocates describe a need to focus policymakers' attention to instances of digital harms felt by the public to add weight to their calls for stronger state-level, legislative protections. One Brussels-based digital rights activist perceived that UK advocates had achieved this more effectively than in Europe, highlighting the examples of the response to the use of algorithms to produce A-level results or the suicidal risks among teenagers.[64] Contrastingly, a number of UK digital rights activists emphasised their difficulty with finding and elevating such case studies into the public eye, beyond the harms experienced by children and publicised by parents and teachers.

Overall, even within resource-rich regions like Europe, there are clear challenges for digital rights organisations when engaging in advocacy efforts to mirror the level of resources of technology companies whose goals can be in direct conflict with digital rights protections.

4.2 DIGITAL RIGHTS AS EMANCIPATION, NOT IN TENSION WITH ECONOMIC GROWTH

There are significant concerns among the digital rights community in both the EU and the UK that the 'rights-model' or an advancement of a digital rights agenda is seen as a barrier to economic growth and innovation.

> *"The sense is that the right balance needs to be struck with digital rights on the one hand and business priorities or economic priorities on the other."*[65]

Critics of the rights-model typically highlight that the US and China lack human rights-based regulation and have the most innovative and largest technology companies e.g. in the form of Meta and Google from Silicon Valley or Baidu or Alibaba from China, something which Europe has struggled to achieve.

However, a direct and causal link between rights-based regulation and dampened innovation is regarded as overly simplistic. Regulation can improve growth, for example, by increasing consumer confidence in an organisation's conduct and products. For this reason, Microsoft's President recently called for regulation of facial recognition technology in the US stressing that if left unregulated, it would unsettle customers.[66] The European Commission has also argued that through the introduction of higher regulatory standards, the EU may capture a commercial advantage as consumers may prefer European AI applications that are easier to trust.[67] Furthermore, a recent report evaluating European competitiveness also highlighted that it was not necessarily the existence of the regulation or human rights protections in the first place that undermined development in the AI field by EU industry actors, but the complexity and level of

63 Quotation from anonymised interview provided by a representative of a digital rights organisation
64 Kolkman, D. (2020) ""F**k the algorithm"?: What the world can learn from the UK's A-level grading fiasco." LSE Blog. https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/
65 Quotation from anonymised interview provided by a representative of a digital rights organisation
66 Smith, B. (2018) "Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility". Microsoft Blogs. https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/
67 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European Approach to Artificial Intelligence, at 2, COM (2021) 205 final

inconsistency in how legislation was being applied across different member states.[68]

Digital rights organisations and academics have also argued that emphasis on digital rights is:

> *"not about attacking Meta and Google; this is about empowering and emancipating people through digital rights."*[69]

> *"I love technology, but it doesn't mean that it has to disrespect us and our rights at the same time, right, we can still develop good technologies, while still respecting people."*[70]

Respondents stressed how digital technologies can facilitate and enable the protection of human rights, such as the use of encryption technology that facilitates privacy online, investment in decentralised digital public infrastructure and the use of AI to fuel social innovation.[71]

A concern about the 'growth narrative' was particularly acute among UK digital rights advocates who had some concerns regarding the new Labour government's emphasis on the centrality of technology to its growth agenda as well as its public reform strategy.

> *"Innovation has been kind of the catch phrase for governments, especially in the UK. But then supposedly if you're critical about some aspect of technology, then people frame you as if you're anti technology. And I think that is something that governments fall for, especially the UK Government."*[72]

Whilst the Minister for the Department of Science and Innovation has stressed the importance of enabling public trust in the technology, the scope of the new UK AI Bill takes a very different path to the EU AI Act. Rather than including all AI systems within its scope, it is limited more narrowly to frontier high risk AI systems. The exclusion of all other AI models from this legislation is felt to signal an aversion to policy approaches that could limit innovation or risk the growth of the technology sector in the short-term.

Overall, there is a clear need for digital rights organisations to highlight how their advocacy is in the interests of or, at the least, will not hinder growth and innovation. The climate justice movement is a key example of a movement that was able to successfully achieve such a strategic repositioning of their goals by highlighting the benefits of 'green jobs' and 'green technology' to the economy. Such a feat could therefore be achievable with the right evidence and advocacy strategies.

4.3 DIGITAL RIGHTS EXEMPTIONS: LAW ENFORCEMENT AND MIGRATION CONTROL

The development of exemptions or second tier approaches for police officials and border controls in new legislation is also felt to undermine digital rights by advocates both in the EU and UK. The exemptions created for certain government departments signal the implication that, unlike fundamental human rights, digital rights are optional or not universally applicable to, for example, migrants or those presumed to have committed crimes. For example, in the EU AI Act, non-EU citizens and migrants entering its territories receive less protections from the testing and use of surveillance technologies than their EU citizen counterparts (see Case Study

68 European Commission (2024) EU Competitiveness: Looking ahead. https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en
69 Anonymous interview with digital rights organisation
70 Anonymous interview with academic
71 Calzada I. (2024) "Artificial Intelligence for Social Innovation: Beyond the Noise of Algorithms and Datafication. 16(19):8638. " Sustainability.
72 Anonymous interview with academic

2b).[73] The Act also allows the use of biometric mass surveillance systems by security officials without the additional safeguards such as fundamental rights impact assessments, high technical standards, and assured anti-discriminatory practice.[74] This particular provision is regarded as a disappointing outcome by digital rights organisations who had advocated for the wholesale prohibition of the technology through the EU AI Act. On the flipside, there have been some successes. In the UK, digital rights groups were successful in their advocacy by proving that an Immigration Exemption in the Data Protection Act 2018 was unlawful.[75] Such examples demonstrate the need for digital rights organisations to persistently demonstrate why migrants and those suspected of committing crimes are also worthy of digital rights protections.

Other examples of exemptions to digital rights for government departments include law enforcement particularly in relation to online platforms. For example, UK's Online Safety Act enables law enforcement to issue a notice to a platform to proactively take down illegal content e.g. Child Sexual Abuse Material (CSAM) which may require breaking end-to-end encryption or enable 'client-side scanning'. Privacy rights groups have regarded this approach as disproportionate government interference and surveillance and thus an infringement on digital rights.[76]

4.4 IMPLEMENTATION AND REDRESS - "BEAUTIFUL WORDS ON PAPER… IT DOESN'T MEAN S***T".[77]

In both the EU and the UK, digital rights activists have emphasised a frustration with the lack of consideration for how new internet laws, such as the GDPR, but also the EU AI Act, are enforced and how a citizen can seek redress if they have experienced harm.[78] Such legislation typically places the burden of enforcement on regulators, yet there are a range of examples of regulators failing to or choosing not to act to enforce existing legislation on behalf of citizens and concerns that the latest legislation will follow suit. This problem is so persistent that the World Economic Forum has emphasised a pervasive 'accountability gap' that must be closed.[79]

In the context of GDPR, recent reports have highlighted how Data Protection Authorities (DPAs) across the EU, particularly in Ireland, have lacked the resources to carry out the full scope of their mandate.[80] This is a renewed concern particularly in relation to enforcement of the AI Act. There is a concern that DPAs resources are spread so thin that they lack the power to fine organisations that refuse to cooperate with their investigations and that they are forced to focus only on a selection of corporate actors whilst turning a blind eye to the state.[81] The recent refusal by ClearView AI to pay fines issued by Dutch, French and Italian DPAs evidences this further and the UK Information Commissioner's Office's (ICO) fine against ClearView was even

73 Rodelli (2023) "The EU AI Act: How to (truly) protect people on the move." Access Now https://www.accessnow.org/eu-ai-act-migration/; Joint Statement. (2024) "EU's AI Act fails to set gold standard for human rights." Algorithm Watch https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf

74 Joint Statement. (2024) "EU's AI Act fails to set gold standard for human rights." Algorithm Watch https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf

75 Open Rights Group (2024) "Why migrants need digital sanctuary". https://www.openrightsgroup.org/blog/why-migrants-need-digital-sanctuary/ ; the3million (2024) "We Won: The immigration exemption to data protection is found unlawful." https://the3million.org.uk/immigration-exemption-unlawful

76 Dewsnip, K. (2023) The Online Safety Act: scrutiny, safeguards and civil liberties. The Constitution Society. https://consoc.org.uk/the-online-saftey-act/#:~:text=Conversely%2C%20not%20all%20of%20the,the%20newly%20created%20criminal%20offences); Index on Censorship. (2024) Our manifesto: the next UK government's necessary actions to restore freedom of expression. https://www.indexoncensorship.org/2024/06/our-manifesto-the-next-uk-governments-necessary-actions-to-restore-freedom-of-expression/; Glitch. (2023) What will the Online Safety Act mean for Black women?: https://glitchcharity.co.uk/what-will-the-online-safety-act-mean-for-black-women/; Article 19 (2024) "New government must prioritise freedom of expression". https://www.article19.org/resources/uk-new-government-must-prioritise-freedom-of-expression/

77 Anonymised quote from an interview with digital rights organisation

78 Access Now (2022) Four years of the GDPR: How to fix its enforcement. https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf; Access Now (2023) Five years of the GDPR: Becoming an enforcement success.https://www.accessnow.org/wp-content/uploads/2023/05/GDPR-5-Year-report-2023.pdf

79 World Economic Forum (2021) https://www.weforum.org/publications/pathways-to-digital-justice/

80 FRA European Union Agency for Fundamental Rights (2024) "GDPR in practice - Experiences of data protection authorities." https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

81 Ibid

overturned on appeal.[82]

There also continue to be scenarios in which fines are not issued to companies despite breaking regulations. For example, in the UK, the ICO merely issued a statement of 'disappointment' when Google announced that it would U-turn on its commitment to block third party cookies used to track user behaviour across different websites on Chrome, despite prior agreements with the Competition Market Authority and the ICO to do so to protect privacy.[83] In its statement, the ICO suggested it would consider regulatory action only if non-compliance was considered systemic over time i.e. beyond just Google.[84] The Open Rights Group has also highlighted a low volume of enforcement activity relating to both state and private sector data protection practice which stands in contrast to counterparts in France who, for example, have issued fines of EUR 150million on Google for its approach to achieving consent for cookies.[85] As a result, the ICO continues to come under fire for a perceived lack of enforcement of data protection law, leaving individuals' privacy and digital rights exposed.[86,87]

An additional concern that also undermines enforcement is a perceived lack of awareness among technology companies regarding how they can comply with regulations. The volume of legislation in the EU combined with the vague or differing definitions e.g. 'gatekeepers' or 'Very Large Online Platforms' between the Digital Markets Act and Digital Services Act, are thought to drive technology companies to disengage from even trying to comply with the legislation. One respondent commended the recent Digital Single Market initiative which seeks to harmonise the rules in the EU, but still felt that *"it doesn't focus on all these aspects in a more coherent, consistent way"*.[88]

These concerns regarding a lack of consideration for implementation and routes for enforcement and redress continue into the EU AI Act with one digital rights advocate emphasising that no lessons were learned from GDPR; *"there wasn't any consideration for how to implement it"* exemplified with a lack of clear definitions here too.

> *"Redress is a huge part of human rights treaties, including the European Charter, but there's nothing to go off there [in the EU AI Act]."*

A particular concern surrounding routes to redress is the lack of awareness among citizens regarding their digital rights and who they should engage with to understand further.

> *"There's still a lot of confusion. Who is responsible for what? So between the ICO and Ofcom… they sometimes work on the same topics, but then it's not really clear who do you then approach if something is wrong?"*[89]

The level of knowledge needed to understand also how to make a claim is also thought to be too technical for the everyday internet user:

> *"If a platform or a person or somebody has done something which overrules your rights. And then you want to complain about it. That requires literacy for people to understand that something wrong has happened. A lot of the definitions are so*

82 BBC (2023) "Face search company Clearview AI overturns UK privacy fine". https://www.bbc.co.uk/news/technology-67133157
83 Google (2024) "A new path for privacy sandbox on the web." https://privacysandbox.com/news/privacy-sandbox-update/
84 ICO (2024) "ICO statement in response to Google announcing it will no longer block third party cookies in Chrome".https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/ico-statement-in-response-to-google-announcing-it-will-no-longer-block-third-party-cookies/#:~:text=%22We%20are%20disappointed%20that%20Google,a%20positive%20step%20for%20consumers.
85 Open Rights Group (2024) "The ICO is leaving an AI enforcement gap in the UK." Open Rights Group. https://www.openrightsgroup.org/blog/the-ico-is-leaving-an-ai-enforcement-gap-in-the-uk/; Open Rights Group (2024). Alternative ICO Annual Report https://www.openrightsgroup.org/app/uploads/2024/11/Alternative-ICO-Annual-Report-Nov-2024.pdf
86 delli Santi (2024) Briefing: The ICO Isn't Working and How Parliament Can Fix It https://www.openrightsgroup.org/publications/briefing-the-ico-isnt-working/
87 Erdos (2022). Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284602
88 European Council, Digital Single Market for Europe, https://www.consilium.europa.eu/en/policies/digital-single-market/
89 Quotation from an anonymised interview with a digital rights organisation

ambiguous and kind of wishy washy that it really doesn't help citizens who want to actually do something about it."[90]

Overall, there remain significant concerns among digital rights organisations in the UK and the EU regarding the lack of forward planning towards how a piece of legislation will be enforced and indeed sufficient funding for such regulators to act. There is also a clear need for renewed efforts to ensure citizens have a complete understanding of their digital rights as well as routes for redress to enable such legislation and its intended protections to be fully actualised.

While resource rich countries and regions struggle with implementation despite their comparative wealth, many nations lack even basic regulatory infrastructure and technical expertise to enforce digital rights protections. This disparity in enforcement capabilities between nations represents a fundamental obstacle at a global level.[91] While UNCTAD has been designated as the focal point for addressing these challenges, particularly in assisting specific countries to improve their participation in the global economy, cross-border enforcement remains a persistent challenge in the digital rights landscape.[92] Even when violations are identified, jurisdictional issues and limited international cooperation mechanisms frequently prevent effective action.[93] Global platforms have been found to implement varying standards of protection across different regions, creating what has been termed a "digital rights divide."[94]

While the United Nations has attempted to address these challenges through frameworks like the Global Digital Compact, implementation remains voluntary and enforcement mechanisms are limited. The latest revision of the GDC has been criticized for its vague formulations and not sufficiently grounding its objectives in international human rights law.[95]

These global challenges directly impact efforts at national and regional levels, as regulators in developed nations struggle to enforce rights protections against companies operating from jurisdictions with weaker oversight. The effectiveness of rights-based regulation continues to be limited by this mismatch between global technology operations and nationally-bounded enforcement capabilities.[96,97]

4.5 DIFFICULTIES DEFENDING COLLECTIVE AND SOCIETAL HARMS

4.5.1 Difficulties defending collective harms in the UK

Among digital rights advocates in the UK, there is a broader concern surrounding the difficulty for advancing human rights claims on behalf of collectives, such as workers or marginalised communities. This challenge goes to the heart of the complexity of how human rights have been historically formulated in defence of the individual, as well as the difficulty advancing a specific legal claim as a collective in a UK court. Such provision is made possible in the EU GDPR because it enables organisations to act on an individual and/or collective's behalf - a provision that was not carried over into the UK version of the bill.

90 Quotation from an anonymised interview with an academic
91 World Ecconomic Forum (2021)'Preventing Digital Harm: World Economic Forum Report Outlines How to Close the Legal and Judicial Gap'https://www.weforum.org/press/2021/09/preventing-digital-harm-world-economic-forum-report-outlines-how-to-close-the-legal-and-judicial-gap/
92 United Nations Conference on Trade and Development (2022) 'Review of capacity-building in and technical assistance on competition and consumer protection laws and policies' https://unctad.org/system/files/official-document/cicplpd31_en.pdf
93 Amnesty International (2024) Global: New technology and AI used at borders increases inequalities and undermines human rights of migrant. https://www.amnesty.org/en/latest/news/2024/05/global-new-technology-and-ai-used-at-borders-increases-inequalities-and-undermines-human-rights-of-migrants/
94 AccessNow (2024)' A pathway forward for digital rights' https://www.accessnow.org/a-pathway-forward-for-digital-rights/
95 (2024)'Unpacking the Global Digital Compact: The Intersection of Human Rights and Digital Governance'https://www.freiheit.org/human-rights-hub-geneva/unpacking-global-digital-compact
96 World Ecconomic Forum (2021)'Preventing Digital Harm: World Economic Forum Report Outlines How to Close the Legal and Judicial Gap'https://www.weforum.org/press/2021/09/preventing-digital-harm-world-economic-forum-report-outlines-how-to-close-the-legal-and-judicial-gap/
97 (2024)'Unpacking the Global Digital Compact: The Intersection of Human Rights and Digital Governance'https://www.freiheit.org/human-rights-hub-geneva/unpacking-global-digital-compact

Such consideration for the needs and experiences of collectives is particularly important in the context of digital rights and technology where harms can be experienced by groups of people as a whole. For example, discrimination as a result of algorithmic bias impacts not just an individual person, but an individual person as a result of their protected characteristics. As a result, any member of a collective who shares such characteristics will also be negatively affected by such an algorithm. Such a conception recognises that a collective can be a 'decision subject' rather than a 'data subject'. A decision subject refers to a group who is subject to decision making systems that make inferences about them - without needing to access or use their own personal data to do so. Specific scenarios of this include, a police force using historic crime data to determine patrol allocations in ways that could increase Stop and Search use in over-policed neighbourhoods, or a social media company removing legitimate online posts in ways that undermine the free expression rights of those interested in LGBTQ+ content.[98] One study has shown that there is less protection for people harmed by automated decision-making in UK law when they are *not* data subjects.[99] This demonstrates that there are particular gaps when harms are indirect and diffuse, such as when arising from algorithmic bias. This gap is further compounded by the lack of transparency surrounding when certain algorithms are used and therefore when such harms could be taking place. Thus, such harms, like algorithmic bias, affect collectives of people, but are difficult to discern and indeed seek remedy for.

4.5.2 Difficulties defending societal harms in the UK and the EU

Societal harms, such as harms to democracy or environmental harms are also a concern among both EU and UK digital rights organisations and academics.

> *"If you look at the way the EU is framing artificial intelligence, or their strategy for artificial intelligence in relation to the environment, it's really like "if we just invest enough in AI, they will figure out a way to get us out of this planet crisis."*

A number of climate justice organisations are now thinking about digital rights because of challenges relating to resource extraction to fuel hardware manufacturing as well as the significant environmental costs incurred by the increase in energy demands by data centres, fuelled by AI.[100] As highlighted by the quotation above, a particular frustration of some digital rights activists is a persistent framing by states that proposes technology as a solution to the environment crisis, such as positioning cloud computing as a solution to sustainability, rather than recognising the ways it forms part of the problem.[101]

Overall, there is a clear appetite among digital rights organisations to raise the profile of collective and societal harms of digital technologies to improve knowledge and awareness of these complexities as well as to explore strategies for more effective digital rights protections.

4.6 RIGHTS INTER-DEPENDENCIES, TRADE-OFFS AND COORDINATION IN UK ADVOCACY

A challenge highlighted solely by digital rights organisations in the UK is the issue of ambiguity regarding how human rights translate into the digital world and indeed what trade-offs would be acceptable when considering all human rights as interdependent.

98 Examples shared in a blog by Connected by Data (2023) "AWO Report: Does the law all non data subjects to challenge algorithmic harms" https://connectedbydata.org/events/2023-09-27-connected-conversation-collective-data-rights
99 Lawrence-Archer & Naik (2023) "Does the law allow non data subjects to challenge algorithmic harm?" https://connectedbydata.org/assets/resources/awo-report-collective-harms.pdf
100 International Energy Agency (2024) Electricity 2024 https://iea.blob.core.windows.net/assets/6b2fd954-2017-408e-bf08-952fdd62118a/Electricity2024-Analysisandforecastto2026.pdf
101 Nioche (2024) The environmental impact of the cloud - the Common Crawl case study. https://www.linkedin.com/pulse/environmental-impact-cloud-common-crawl-case-study-julien-nioche-at8xf

Interestingly, a number of digital rights advocates suggested that they considered this a unique problem to the UK context compared to the EU. Advocates feel there is a greater understanding among EU policymakers and EU civil society of the need to consider how to achieve protections for all human rights, noting their inter-dependencies, through an enabling environment. This was felt to be the case in part because of the EU Digital Rights and Principles framework – though some UK digital rights advocates were less familiar with it – but even more so because of a broader culture of support for holistic human rights frameworks norms across the EU.

In the UK, by contrast, there is a concern that firstly, the language of rights is much less common and compelling because of the recent hostility surrounding the human rights agenda by the former Conservative government. This was reflected by attempts to repeal the Human Rights Act and to weaken ties to the European Court of Human Rights (ECHR).[102] As a result, a number of civil society groups interviewed throughout this research suggested that they have actively avoided the language of rights in recent history.

Secondly, there is a felt ambiguity regarding how exactly human rights translate into digital rights holistically in the UK stemming from a perception that many UK human or digital rights organisations view specific rights in siloes. For example, children's rights and safety will be approached as the sole or priority goal for intervention, without consideration of the trade offs for privacy or freedom of expression, or vice versa. There were notable examples of organisations and advocates who were explicitly named as exempt from this critique, but the reflection on challenges faced by the broader digital rights movement as a whole was nonetheless mentioned by a significant number of respondents in the UK.

There are clear examples of strong collaboration and networked mobilisation across UK civil society, including during the Online Safety Bill, and now as new coalitions have emerged.[103] However, some advocates highlighted concerns that there remain different clusters of civil society organisations that have strongly divergent goals, even within, for example those who advocate for freedom of expression. Such divergence may have contributed to why some describe the Online Safety Act as a 'Christmas Tree Bill' with something there for everyone, but very little coherence. For example, there was a provision for the protection of news publisher and journalistic content in relation to content moderation and complaints procedures as a nod to those passionate about freedom of expression, yet this caused frustration among those with concerns about the misinformation laden in legacy media and the lack of protection for citizen journalists who, as one respondent put it, *"would be subject to higher levels of online censorship"*. Or the commitment to age assurance mechanisms and illegal content takedown notices as a nod to those concerned about children's safety, despite the potential infringements this created for those concerned about privacy rights and breaking end-to-end encryption.[104,105,106] Please see Appendix: Case Study 2 for a summary of the different areas of the Online Safety Act that are celebrated and lamented by digital rights organisations.

102 Ministry of Justice, UK Government (2022) Bill fo Rights to strengthen freedom of speech and curb bogus human rights claims https://www.gov.uk/government/news/bill-of-rights-to-strengthen-freedom-of-speech-and-curb-bogus-human-rights-claims

103 The Online Safety Act Network and the Data & AI Civil Society Network led by Connected by Data are notable examples in the UK

104 DSIT and Home Office. The Online Safety Act Impact Assessment. 2024. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf; Hern, A. (2024) What is the UK's Online Safety Act and what powers will it provide? The Guardian :https://www.theguardian.com/law/article/2024/aug/08/what-is-uk-online-safety-act-new-legislation-laws; Judson (2022) The Online Safety Bill, Demos Position Paper. Demos. https://demos.co.uk/wp-content/uploads/2023/02/OSB-position-paper.pdf

105 Dewsnip, K. (2023) The Online Safety Act: scrutiny, safeguards and civil liberties. The Constitution Society https://consoc.org.uk/the-online-saftey-act/#:~:text=Conversely%2C%20not%20all%20of%20the,the%20newly%20created%20criminal%20offences); Index on Censorship. Our manifesto: the next UK government's necessary actions to restore freedom of expression. 2024. https://www.indexoncensorship.org/2024/06/our-manifesto-the-next-uk-governments-necessary-actions-to-restore-freedom-of-expression/; Glitch. (2023) What will the Online Safety Act mean for Black women?: https://glitchcharity.co.uk/what-will-the-online-safety-act-mean-for-black-women/; Article 19 (2024) "New government must prioritise freedom of expression". https://www.article19.org/resources/uk-new-government-must-prioritise-freedom-of-expression/

106 Commission Nationale Informatique & Libertes (2022) "Online age verification: balancing privacy and the protection of minors". https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

Human and digital rights advocates indicated that significant 'definitional work' is needed between civil society groups engaging in tech policy in order to clarify and agree shared views of what different human rights mean in an online context and where the consensus lay on what compromises should be made for achieving their protections. One example of this is the potential interpretation of freedom of speech online as also meaning what some refer to as 'freedom of reach' i.e. someone should have a right to amplify their speech to millions of people. Yet, some would argue that freedom of speech online does not mean you should automatically be entitled to such a platform. A further example of such ambiguity in definitions is whether you might consider social media platforms 'shadow banning' certain minoritised groups online is an infringement on freedom of speech.[107] Yet, some might argue that it is a false equivalence.

> *"It feels like, as a policy collective, we haven't got down to that granular detail yet. We can talk very broadly about how we care about freedom of expression online. We care about privacy online… but when it really gets to OK - how does that make a difference to whether we endorse this tech policy or that tech policy -that's when it starts coming apart."*[108]

This need for a more detailed conversation regarding the goals of UK civil society groups in relation to digital rights protections was felt to also be useful for a range of purposes, not just to facilitate more detailed, precise and impactful advocacy that could avoid vague proposals, such as which content should be removed and on what basis. It could also facilitate the prioritisation of efforts when resources are spread thin across a multiplication of bills and policy approaches. A sense of prioritisation and networked power was also thought to be useful for funders considering how best to support the scale-up of existing efforts.

4.7 DIGITAL ACCESS AND SKILLS - A DIVERGENCE BETWEEN THE UK AND WIDER WORLD

Digital inclusion charities in the UK have highlighted a range of challenges with both digital access and skills development that relate, but do not mirror to the same extent, the broader concerns at a global level (as highlighted above when discussing the global digital divide). The specific and persistent challenges with accessibility and affordability of digital devices and connections as well as basic digital skills are highlighted in Appendix: Case Study 4.

However, interestingly, the context in which digital access and skills was raised in the UK among digital rights organisations and academics was more in relation to understanding other digital rights and how to seek remedy for harms such as infringements on privacy, rather than regarding digital access and participation in technological development as a digital right in its own right. This stands in contrast to digital rights norms and principles at a global level and those emerging within the EU where accelerating digital access and skills, including participation in technological development, has also become a priority. Therefore, whilst there is awareness and significant focus on tackling digital access, skills and participation in technological development as a need among civil society and potentially a right in the UK, it does not currently appear to be a challenge prioritised by digital rights organisations in the UK specifically. Instead, this policy area is championed by different organisations in a distinct network, such as economic justice organisations and internet industry partners, such as, for example in the UK, Good Things Foundation, the Digital Poverty Alliance or FutureDotNow. This separation suggests that the UK remains an outlier and distinct from global transformations in conceptualisations of digital access.

107 Washington Post (2024) "What is shadowbanning"? https://www.washingtonpost.com/technology/2024/10/16/shadowban-social-media-algorithms-twitter-tiktok/
108 Anonymous interview with digital rights organisation

5. OPPORTUNITIES FOR ADVANCING DIGITAL RIGHTS

There are a range of opportunities for strengthening digital rights protections at national, regional and a global level in 2025, presented here:

5.1 UK OPPORTUNITIES

As set out by the Minister for the Department of Science, Innovation and Technology, Peter Kyle:

"The future of technology is ours to shape, and the opportunities it offers are ours to seize."[109]

At the close of 2024, we have a new government that envisions "a future where technology enriches the life of every single citizen" and that offers "unequivocal" support for human rights.[110] The AI Opportunities Action Plan also emphasises "the importance of fostering public trust in technology, particularly considering the interests of marginalised groups."[111] We recommend that the UK government facilitates this vision by developing and declaring a set of Digital Rights & Principles. Such a declaration would not be legally binding in order to avoid adding additional complexity and incoherence to existing regulation. Instead, it would act as a set of foundational and organising rights and principles with which to both cohere, explain and identify gaps in existing policies and legislation, as well as to inform and motivate new policies and legislation relating to technology.

Through its development, if conducted via a deliberative process supported by policymakers and informed by the expertise of digital rights experts and technologists, we can better understand and reflect the needs, values and priorities of citizens and, as a result, enable citizens to truly understand and shape the future of technology.

109 Peter Kyle (2024) "Technology in Public Services. Volume 753: debated on Monday 2 September 2024." UK Parliament. https://hansard.parliament.uk/commons/2024-09-02/debates/721F0511-796C-49C4-A4FF-E0528E6419C6/TechnologyInPublicServices
110 Ibid; Attorney General's Office (2024) Attorney General's Bingham Lecture on the rule of law https://www.gov.uk/government/speeches/attorney-generals-2024-bingham-lecture-on-the-rule-of-law;
111 DSIT (2025) "AI Opportunities Action Plan." https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

In 2025, we will see a new wave of digital policy and legislation – from the Data Use and Access Bill, the Fraud, Debt and Error Bill and the Artificial Intelligence Bill, to cross-departmental policies such as the use of AI to accelerate productivity in public service reform and a new digital inclusion strategy. Clarifying citizens' foundational digital rights and protections in a holistic framework is therefore an urgent task to support and guide this work.

We see six key benefits for investing in the development and Declaration of Digital Rights and Principles for the UK:

A. **Citizen trust:** Citizens can gain stronger foundations for trusting that the technology they interact with, particularly when deployed in public services, is designed, developed and deployed in a way that respects their rights. Such trust, if fairly earned, will better enable the goals of deploying such technology in public service reform.

B. **Citizen empowerment:** The work to develop a digital rights framework will provide opportunities to refine and clarify the language of digital rights with citizens providing a stronger platform to facilitate discussions about how the public can protect themselves online and behave responsibly. It will also provide a platform for explaining where and how such digital rights may already be protected via existing legislation, how citizens can best seek remedy if they find their rights have been abused, as well as identify where gaps in existing legislation and policy remain.

C. **Technological innovation:** Technologists have a clearer sense of the guardrails citizens' need assurances when designing new technologies for the long term to support their adoption and use.

D. **Policy and regulatory coherence:** The UK government will have a clear and coherent framework to align, communicate and evaluate existing policy and legislation against - providing a platform to tackle the contradictions and ambiguity of the status quo.

E. **Stronger civil society collaboration and alignment:** By focusing on developing a singular holistic digital rights framework, digital rights organisations will have a shared opportunity to clarify, align and consolidate their advocacy around. From a resourcing perspective, providing such organisations are supported to participate in such an exercise, this could help minimise being spread thin across the proliferation of digital policy development presented by government and technological innovation across the wider world and provide a stronger footing on what is already an uneven playing field relative to lobbyists in the technological industry. It also provides an opportunity for a united and therefore strengthened position for a higher volume of civil society organisations to advocate with.

F. **Regional and global partnerships:** The UK will have a stronger footing to strengthen partnerships with other countries who are accelerating digital rights protections, providing a more joined up regulatory environment that can better facilitate growth and innovation as well as universal digital rights protections regardless of citizenship status.

The following opportunities present the ground-work to support a citizen-led process for the development of a digital rights framework and a new Declaration of Digital Rights & Principles in the UK, with additional intermediary benefits in the process of its development.

Recognising how resource and time poor digital rights organisations in the UK already are, any opportunities targeting such organisations are also written for funders exploring routes to systemically facilitate stronger digital rights protections for citizens.

5.1.1 Establish and nurture a UK digital rights network: Drawing on wider digital rights as well as social, racial and economic justice organisations, funders could enable a regular opportunity for such organisations to convene as a network to meet, share knowledge and align on priorities across the breadth and diversity of digital rights and shared goals that, crucially, include organisations targeting digital access, skills and participation in technological development.

To enable this network to thrive and for social, racial and economic justice organisations to participate, funders should also consider funding and facilitating an educational programme for any UK-based social, racial or economic justice organisations interested in expanding expertise and confidence to incorporate digital dimensions into their work. Draw on the Digital Freedom Fund's 'Digital Rights For All' programme as an example.[112]

5.1.2 Clarify digital rights language: Drawing on the digital rights network (1.1) as an advisory and guiding body, funders should invest in qualitative research with the public, particularly with different marginalised communities, to explore and clarify the language that could be used to discuss and define digital rights. Particular consideration should be given to the variety of connotations and associations such complex concepts can have such as what it means to have free expression in an online environment or to have equal protection against discrimination. Draw on tools such as the 'Talking Digital' lexicon to help inform discussions.[113] This step will be an important foundation for facilitating a deliberative process with the public to develop a digital rights framework.

5.1.3 Develop a UK digital rights framework through a deliberative process: The UK government and/or other funders should invest in a deliberative process with the public to identify and refine the priorities for a cohesive digital rights framework. The deliberations should:

- Utilise the clarified language for digital rights (1.2) and draw on the expertise of digital rights network (1.1), UK policymakers as well as technologists where needed to inform and shape the design of the overall process and discussions within it. The breadth and inclusivity of the deliberation's design will be crucial to its ultimate success.
- Ensure they are sufficiently funded so that digital rights organisations and citizens can participate to avoid power disparities
- Build on examples such as the Global Digital Compact, EU's Declaration of Digital Rights and Principles and South Korea's Digital Bill of Rights and consider alignment with global rights and principles to ensure such a framework avoids excluding those globally disproportionately affected by digital rights abuses

The outcome of this deliberation, a citizen-led digital rights framework, can then be used by the digital rights network (1.1) to facilitate and guide priorities for advocacy for a UK Declaration of Digital Rights and Principles.

5.1.4 Digital rights coalition to coordinate a united communications campaign: Given the known tension between digital rights protections and growth and innovation, the new digital rights coalition could consider developing a united strategic communications campaign, ideally, if possible, in collaboration with partners in the technology industry, that highlights why digital rights protections should not and does not limit or undermine innovation and growth. Such a campaign could support the adoption for a new UK Declaration of Digital Rights and Principles.

112 Digital Freedom Fund (2021) Digital Rights for All. https://digitalfreedomfund.org/digital-rights-for-all/
113 Digital Freedom Fund. Talking Digital: A Lexicon by Digital Freedom Fund. https://digitalfreedomfund.org/wp-content/uploads/2022/12/WEB-03102022_TALKING-DIGITAL-LEXICON_150DPI.pdf

5.1.5 The UK government, drawing on the Department for Science, Innovation, and Technology (DSIT) as the coordinating department, should adopt a citizen-led Declaration of Digital Rights and Principles.[114] This adoption could be borne out of initial support and involvement in the deliberative process, either/ both as a funder and an influencer in the design and parameters of the discussion. The government, through DSIT, could then use such a Declaration to:

- Evaluate existing policy approaches to identify gaps and opportunities for improving digital rights protections for citizens.
- Invite colleagues as well as in other departments such as the Department for Education and the Department for Work and Pensions to highlight potential new policy approaches for strengthening digital rights protections and what goals might be achievable in the course of this and the next Parliament.
- With the support of the Digital Regulation Cooperation Forum, invite regulators, including Ofcom, Information Commissioner's Office, Competition and Markets Authority and the Financial Conduct Authority, to communicate how their existing regulatory efforts facilitate the Digital Rights & Principles included in the Declaration.
- Share annual progress reports towards digital rights protections goals over the course of this and the next Parliament.

5.2 REGIONAL OPPORTUNITIES FOR EUROPE AND OTHER REGIONS

Whilst the following opportunities could largely apply to any regional bodies, these opportunities are written specifically for European policymakers.

5.2.1 Explore how the new EU 'Digital Rights and Principles' could be incorporated into existing European rights legislation e.g. via an amendment to the European Convention on Human Rights or the European Charter using an approach that would avoid disrupting existing case law relating to the original versions.

5.2.2 Strengthen digital collaboration by expanding regional partnerships. For example, the 2019 EU-AU Digital Economy Task Force set goals for a shared digital economy, leading to the EU-AU Partnership on Digital Transformation and the EU-AU Data Flagship. Similar efforts, such as the Digital4Development (D4D) Hub for Latin America and the Caribbean, foster human-centered digital transformation.[115] Broadening these partnerships enables the EU to co-create inclusive, secure, and sustainable digital infrastructures and governance frameworks.

5.2.3 Enhance advocacy through coordinated funding mechanisms. Smaller digital rights organizations face challenges in policy advocacy due to limited resources and the lobbying power of large tech companies. Coordinated funding, as seen with initiatives like the Digital Freedom Fund (DFF), allows these groups to align strategies and amplify their impact across regions. Expanding such funding models globally would enable more organisations to advocate for cohesive digital rights protections, creating a stronger, unified front in policy discussions.

5.2.4 Regional bodies could establish coordinated monitoring frameworks to track and enforce digital rights protections across member states. Similar to the EU's digital principles monitoring system, these frameworks would provide shared guidelines, metrics

114 We recognise concerns regarding whether DSIT is sufficiently resourced and/or indeed the right department to situate this work given the breadth of the digital rights framework's scope. We welcome input and feedback for whomever is best placed within the UK government to own and coordinate this initiative.

115 European Commission (2024) "Digital For Development Hub for Latin America and the Caribbean" https://international-partnerships.ec.europa.eu/policies/global-gateway/digital-development-d4d-hub-latin-america-and-caribbean_en

and enforcement mechanisms to reduce fragmentation and ensure consistent application of standards.[116] A unified monitoring approach would strengthen oversight while supporting states with practical tools and shared data for identifying issues early and coordinating responses. By standardising how protections are tracked and upheld, regions can more effectively advance digital rights through data-driven, collaborative enforcement.

5.3 GLOBAL OPPORTUNITIES TO ADVANCE DIGITAL ACCESS

5.3.1 The UN could establish and coordinate a Global Fund for Digital Infrastructure as proposed by the Global Digital Compact. This fund should focus on bridging digital divides by supporting secure, accessible, and resilient digital infrastructure in underserved regions, promoting equitable access aligned with global digital rights principles. The UK and EU should actively contribute funding and expertise to shape this initiative.

5.3.2 UNESCO, working with regional bodies, could implement AI readiness assessments within participating regions, building on its existing Readiness Assessment Methodology. This opportunity supports countries in developing frameworks and regulatory capacities that align with digital rights principles, ensuring inclusivity and local relevance.

5.3.3 The UN could establish a global framework that standardises data access for research and platform oversight. Working with UNESCO's ethical principles and the G7's data cooperation roadmap, this framework should establish standards for cross-border data sharing, research access, and privacy protections.[117] The OECD and ASEAN-EU collaboration models demonstrate how coordinated governance can balance research needs with privacy rights while ensuring consistent implementation across jurisdictions.[118]

5.3.4 International organisations, particularly the UN and ITU, could design digital access initiatives that explicitly address structural power imbalances in connectivity and infrastructure. Following the principles outlined in the Global Digital Compact and UNESCO's ethics recommendations, these initiatives could focus on inclusive collaboration, capacity-building, and shared responsibility. By centering digital development on fairness and accountability, global policies would help ensure that underrepresented regions benefit from and contribute to the digital ecosystem on equal terms.

116 European Commission: Directorate-General for Communications Networks (2024) "Content and Technology, Study to support the monitoring of the Declaration on Digital Rights and Principles – Final report", Publications Office of the European Union https://data.europa.eu/doi/10.2759/875696

117 G7 United Kingdom (2021) "G7 Roadmap For Cooperation On Data Free Flow With Trust". https://assets.publishing.service.gov.uk/media/609cf5e18fa8f56a3c162a43/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf

118 Helleputte and Aw (2024) "ASEAN and EU Finalise Implementation Guide for Cross-border Data Transfers". Privacy World. https://www.privacyworld.blog/2024/02/asean-and-eu-finalise-implementation-guide-for-cross-border-data-transfers/

CONCLUSION

This paper concludes at a pivotal moment in the evolution and normalisation of digital rights and principles and for UK technology policymaking.

The extension of existing human rights into the digital world and development of wholly new digital rights, such as universal digital connectivity and the ability to participate in technological development, represents an opportunity to clearly articulate the specific protections and policies needed to enable the basic rights and freedoms that all people are entitled to. The importance of ensuring such new rights are developed and articulated in a way that is inclusive of and reflective of the priorities of those most at risk of harm and avoiding tech-centric solutions to prevent them is clearly at the forefront of the minds of digital rights activists.

The recent establishment of global norms and principles surrounding ethical AI development as well as reconceptualisation of digital access to include skills and participation in technological development presents additional opportunities for new digital rights at a national and regional level. The decolonisation agenda underway within the digital rights movement in the EU and the UK has also driven greater focus on the needs of marginalised communities, particularly migrant communities, and forms of collective harms, both with the UK and EU as well as at a societal level, through environmental harms. When combining such progression with the demands of engaging with rapid technological and sequentially legislative development, it is no surprise that the energy and resources of the digital rights movement is spread too thin.

However, digital rights advocacy faces a number of additional challenges that diverge and overlap between EU and UK advocates. Within both the EU and the UK, digital rights advocates highlighted:

- An 'uneven playing field' between digital rights advocates and technology companies when advocating for digital rights protections to states.
- It is a struggle to demonstrate that digital rights goals are not in tension with economic growth and innovation.
- States are too frequently making exemptions to their protections of digital rights in legislation to empower law enforcement and border control which undermines the fundamental principle of human rights being applicable to all equally.
- Legislative efforts too rarely take approaches for enforcement and redress into account in their development resulting in a devaluing of the power of these laws and an inability for citizens to seek remedy.
- There are insufficient protections for societal harms such as the impact of technology on the environment.

UK digital rights advocates in particular also highlighted that:

- There are currently insufficient protections and routes to redress for collectives such as minority ethnic communities or workers despite there being distinct harms that can be produced and exacerbated by technologies that affect such groups, such as algorithmic bias.
- There is a lack of coordination and joined up advocacy within the UK digital rights movement which is resulting in different digital rights organisations advocating for protections and goals in a siloed way, that can clash and produce corresponding infringements in the final negotiated legislation.
- Digital access and skills whilst a key policy area and priority for digital inclusion charities in the UK is not currently conceived as a 'digital right' or traditionally considered part of the digital rights movement - despite this being a key feature of the movement at a global level and more recently within the EU.

There are clearly significant opportunities for strengthening digital rights protections both for advocates and policymakers, nationally, regionally and globally, in 2025, including (but not limited to):

- Digital rights organisations uniting and leading the development of a digital rights and principles framework through a deliberative process with citizens to align, strengthen and guide advocacy in the UK, that could include digital access, skills and participation in technological development
- UK policymakers in the Department for Science, Innovation and Technology to adopt a recommended digital rights framework as a new Declaration of Digital Rights & Principles to help guide technological progress and to identify gaps in existing legislation and policy to inform new development, as well as to monitor progress across the government towards its goals
- The European Union to strengthen digital collaboration by expanding regional partnerships to co-create inclusive, secure and sustainable digital infrastructures and governance frameworks
- The UN to establish and coordinate a Global Fund for Digital Infrastructure as proposed by the Global Digital Compact
- International organisations, like the UN and ITU, to design digital access initiatives that explicitly address structural power imbalances in connectivity and infrastructure

APPENDIX
POLICY AND LEGISLATIVE APPROACHES CASE STUDIES

This Appendix collates in-depth digital rights based analysis of a selection of specific EU and UK digital policy areas and legislation, namely:

1. Data privacy
2. Balancing freedom of expression and online safety on social media platforms
3. Human-centric digital technology development
4. Digital skills
5. Digital access

In each section, we first, focus on the EU and UK by:

- Introducing a specific aspect of the European Declaration of Digital Rights and Principles that is most pertinent to the policy area and area of digital rights
- Discussing a sample of relevant policies or laws in the EU and the UK in detail through a digital rights lens. This is to facilitate consideration for how new digital rights and principles can be used to evaluate pre-existing digital policies.

Second, we turn to a global lens by sharing how these UK and EU policy areas or laws relate back to emerging global principles via the Global Digital Compact and, in some cases, the Council of Europe Treaty, as well as the new Digital Bill of Rights recently introduced by the Republic of South Korea.

- We also provide the global principles as well as commitments via the Council of Europe Treaty to highlight other global influences on policy making.
- We use the South Korean Digital Bill of Rights and surrounding policy as an example of a national framework of the sort the UK may consider developing in the future.

Due to time and space constraints, this section of policy and legislative approaches is by no means exhaustive of all digital rights or indeed all policy approaches taken by the UK government or EU that relate to digital rights. It was also completed in November 2024 and therefore does not include a number of the policy developments launched between December 2024 and February 2025 such as the Data Use and Access Bill.

Instead, this section serves to exemplify the types of progress towards digital rights protections that have already been made in the UK and EU, recognising that much of this progress was also not designed with the explicit purpose of achieving such protections. Opportunities for further extending digital rights protections are included in Chapter 5 above.

CASE STUDY 1
DATA PRIVACY

As highlighted in Chapter 3, the right to privacy surrounding personal data and online surveillance was a key platform for mobilisation for the digital rights movement in the EU. It is therefore not surprising to see it represented in the European Union's Declaration of Digital Rights and Principles.

In this section, we evaluate a subsection of policies that relate to data privacy in the EU and the UK before turning to reflect how such principles are discussed in South Korea's Digital Bill of Rights and in the Global Digital Compact.

CS 1.1 European approaches

In the European Declaration of Digital Rights and Principles, it stipulates that:[119]

- Article 17: Everyone has the right to privacy and to the protection of their personal data. The latter right includes the control by individuals on how their personal data are used and with whom they are shared.
- Article 18: Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and not to be subjected to unlawful online surveillance, unlawful pervasive tracking or interception measures.

To enable this, the EU commits to, for example:

- Ensuring that everyone has effective control of their personal and non-personal data in line with EU data protection rules and relevant EU law;
- Ensuring that individuals have the possibility to easily move their personal and nonpersonal data between different digital services in line with portability rights;
- Effectively protecting communications from unauthorised third party access;
- Prohibiting unlawful identification as well as unlawful retention of activity records.

119 European Commission (2022) "European Declaration on Digital Rights and Principles". Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

In the EU, the cornerstone General Data Protection Act (GDPR) lays down rights and obligations to facilitate control of personal data. It came into effect for EU Member States in 2016 and sets out how personal data should be 'collected for specified, explicit and legitimate purposes' and 'processed lawfully, fairly and in a transparent manner'.[120,121] It also sets out how data should be 'handled, accessed and shared by organisations across the EU'.[122] The ePrivacy Directive also provides for the protection of the confidentiality of communications and related traffic data.[123]

All member states have implemented the GDPR and ePrivacy Directive and many run educational programmes, often co-funded by the EU, to educate citizens on their rights concerning data protection. Some member states also have technical solutions to enabling data privacy. For example, Estonia has implemented a data tracker which allows citizens clear access to an overview of operations being performed with their data. It's designed to interface with public sector information systems that store and process their personal data.[124] Despite these measures, challenges remain with a relatively low proportion of European citizens regarding their privacy online is well protected (51%).[125]

UK approaches[126]

The UK's Data Protection Act 2018 supplemented the EU GDPR laws, incorporating these regulations into a UK context.[127] The DPA 2018 built on the UK's original Data Protection Act of 1998.[128] Following the Brexit referendum and the subsequent enactment of the European Union (Withdrawal) Act 2018, the EU GDPR continued to apply in the UK throughout the transition period until the end of 2020.[129] From 1st January 2021, the GDPR has been retained in domestic law as the UK GDPR, alongside the DPA 2018.

Since 2021, the EU commission has adopted adequacy decisions for the UK GDPR, meaning that in the majority of cases, "data can continue to flow freely from the EU to the UK".[130] However, to maintain adequacy, the UK must continue to provide an "essentially equivalent" level of data protection, which is monitored by the EU Commission.[131] Data adequacy with the EU is a topic of political debate in the UK, as the British government has continued to take steps to diverge from GDPR.[132]

120 Longstaff, G (2024) "The importance of data privacy law in the digital age". https://www.law.ac.uk/resources/blog/the-importance-of-data-privacy-law-in-the-digital-age/.
121 Joint Committee on Human Rights (2017) "Note from Deputy Council: the Human Rights Implications of the Data Protection Bill". https://www.parliament.uk/globalassets/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf
122 Ibid.
123 European Union (2002) "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)". https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.
124 Republic of Estonia Information System Authority "Data tracker". https://www.ria.ee/en/state-information-system/people-centred-data-exchange/data-tracker.
125 Special Eurobarometer 551 (2024) "The Digital Decade". https://digital-strategy.ec.europa.eu/en/news-redirect/833351.
126 Please note this section was written while the Data Use and Access bill was in the process of being amended in the House of Lords and therefore was not included in our analysis.
127 Ibid.
128 The National Archives (2018) "Data Protection Act". https://www.legislation.gov.uk/ukpga/2018/12/enacted
129 Information Commissioner's Office (2020) "Information rights at the end of the transition period Frequently Asked Questions". https://ico.org.uk/media/for-organisations/documents/2617966/information-rights-and-eot-faqs.pdf.
130 Information Commissioner's Office, Overview – Data Protection and the EU. https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/#:~:text=About%20this%20guidance,has%20an%20approved%20adequacy%20decision.&text=What%20does%20adequacy%20mean?,What%20about%20law%20enforcement%20processing?
131 Ibid.
132 Delli Santi, M. (2021) "UK Adequacy: it's only the beginning". Open Rights Group. //www.openrightsgroup.org/blog/uk-adequacy-its-only-the-beginning/.

The following Table 1 captures the strengths and weaknesses of GDPR in the UK through the lens of digital rights. Enabling factors such as transparency, enforcement and remedy are colour coded throughout the table.

TABLE 1
STRENGTHS AND WEAKNESSES OF GDPR IN THE UK THROUGH THE LENS OF DIGITAL RIGHTS

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Freedom of information	The right of access of the data subject is introduced in Article 15 of the GDPR. The Right of access allows a data subject to confirm if their personal data is being processed, and if so, the category of personal data and the purpose for which it is being processed.[133] The Right of access to one's own personal information is an enabling right, allowing for the exercise of other rights. The GDPR removed practical barriers to its exercise, such as the payment of fees.[134]	There is concern that the Right to access one's own personal data may conflict with the practice of Data protection by design, which is set out in Article 25 of the GDPR.[135] This conflict may arise when a company uses technical measures such as pseudonymisation and data compartmentalisation to ensure that data cannot be linked to a named individual.[136] In this case, a person trying to access this data may be unable to, even if it is their own personal data. While GDPR requires the data controller to provide "meaningful information about the logic involved" in an algorithm which utilises an individual's personal data to make decisions, the data controller is not required to disclose the full algorithm.[137]

133 Intersoft consulting (2018) "General Data Protection Regulation: Article 15". https://gdpr-info.eu/art-15-gdpr/.
134 Johnson-Williams, E. (2018) "Debates, awareness, and projects about GDPR and data protection". Open Rights Group. https://www.openrightsgroup.org/publications/debates-awareness-and-projects-about-gdpr-and-data-protection/#h.7jr28z5qizxn
135 Ruiz, J. (2018) "The right of access in GDPR: What are the debates?". Open Rights Group. https://www.openrightsgroup.org/blog/the-right-of-access-in-gdpr-what-are-the-debates/.
136 Ibid.
137 Cloisters (2020)"AI Law Consultancy, Artificial Intelligence, Machine Learning, Algorithms and Discrimination Law: The New Frontier". https://global-uploads.webflow.com/5f57d40eb1c2ef22d8a8ca7e/606710cc05a1b6228ae758fc_Discrimination-Law-in-2020.FINAL_-1.pdf.

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Privacy	Articles 16 - 19 of the GDPR introduce the Rights to rectification, Right to erasure and Right to restriction of processing, as well as a Notification obligation regarding any of these rights. These articles mean that a data subject has the right to request for their personal data to be corrected if there are any mistakes, erased if the data is no longer needed and/or consent has been withdrawn, and to restrict the processing of personal data for the same reasons. Under Article 19, a data controller is obligated to inform a data subject if any of the actions described in Articles 16 - 18 is carried out on their personal data.[138] Article 25 of the GDPR introduces the principle of Data protection by design and by default.[139] Under Article 25, data controllers must implement data-protection principles, such as data minimisation, and appropriate technical and organisational measures, such as pseudonymisation.[140]	The Information Commissioner's Office (ICO) is the UK's independent regulator for data protection, which includes both GDPR and DPA 2018. The ICO has come under fire for a perceived lack of enforcement[141] of data protection law, leaving individuals' privacy and digital rights exposed.[142] Article 21 of the GDPR introduces a Right to object to the processing of one's personal data. However, this protection is limited when data is processed by the public sector, or by an organisation which claims a "legitimate interest", which may put the burden of proof on the individual to demonstrate harm to "specific interests and freedoms".[143] The Exemptions for political parties, set out in Schedule 1, Paragraph 22 of the DPA 2018, allows political parties to process personal data revealing political opinions, without the individual's consent, for the purposes of political activities and democratic engagement.[144] Critics argue that this provision enables exploitation of personal data by third parties, including targeted political advertisements.[145] Similar exemptions exist for national security and intelligence services.

138 Intersoft Consulting (2018) "General Data Protection Regulation, Article 19". https://gdpr-info.eu/art-19-gdpr/.
139 delli Santi, Mariano (2022) "Analysis: The UK Data Protection and Digital Information Bill". Open Rights Group. https://www.openrightsgroup.org/publications/analysis-the-uk-data-protection-and-digital-information-bill/
140 Ibid
141 delli Santi, Mariano, Briefing: The ICO Isn't Working and How Parliament Can Fix It (2024). https://www.openrightsgroup.org/publications/briefing-the-ico-isnt-working/
142 Erdos, David, Towards Effective Supervisory Oversight? Analysing UK Regulatory Enforcement of Data Protection and Electronic Privacy Rights and the Government's Statutory Reform Plans (2022). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4284602
143 Johnson-Williams, Ed, Debates, awareness, and projects about GDPR and data protection (2018). https://www.openrightsgroup.org/publications/debates-awareness-and-projects-about-gdpr-and-data-protection/#h.7jr28z5qizxn
144 Privacy International, UK Data Protection Act 2018 – 339 pages still falls short on human rights protection (2018). https://privacyinternational.org/news-analysis/2074/uk-data-protection-act-2018-339-pages-still-falls-short-human-rights-protection
145 Ibid.

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Protection from discrimination	Article 22 of the GDPR establishes the Right not to be subject to solely Automated Decision Making, including profiling. There is well-established evidence of bias and discrimination being replicated within algorithms as the result of biassed training data, including in Automated Decision Making systems.[146] As set out by Article 35 of the GDPR, organisations are required to do a Data Protection Impact Assessment (DPIA) when they use personal data in a high-risk way.[147]	Private companies providing Live Facial Recognition services have used the "substantial public interest" provision in the GDPR to justify their processing of biometric data, which includes scanning the face of every customer entering a given store, as well as creating and sharing watchlists of suspected shoplifters.[148] Law firm AWO has argued that this case is an improper use of the provision of "substantial public interest".
Equality of human rights	As of 8th March 2024, following a Court of Appeal decision, the Immigration exemption to UK GDPR and the DPA 2018 was amended to add additional safeguards, including a "balancing test" to ensure that the "risk to immigration control is substantial and outweighs the risk to the person's interests", making a record of the exemption and the reasons for making the decision, and informing the data subject.[149]	The Immigration exemption in the DPA 2018 has come under substantial criticism for treating the human rights of non-UK citizens as lesser to those of UK citizens.[150] Critics remain concerned that the burden to exercise one's rights when an improper use of the exemption is believed remains on the individual.[151]

146 Data (Use and Access) Bill: European Convention on Human Rights Memorandum (2024). https://bills.parliament.uk/publications/56595/documents/5246.
147 Equality and Human Rights Commission, Personal data rights in the Data Protection and Digital Information Bill (2024). https://www.equalityhumanrights.com/media-centre/blogs/personal-data-rights-data-protection-and-digital-information-bill
148 AWO, Big Brother Watch: complaint against private sector facial recognition (2022). https://www.awo.agency/blog/big-brother-watch-complaint-against-private-sector-facial-recognition/
149 Information Commissioner's Office, Immigration exemption: a guide (2024). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/
150 Open Rights Group, "Immigration exemption" ruled unlawful under GDPR (2021). https://www.openrightsgroup.org/campaign/immigration-exemption-campaign-page/
151 Alsherif, Sara, Government does the bare minimum to update the Immigration Exemption (2024). https://www.openrightsgroup.org/blog/government-does-the-bare-minimum-on-the-immigration-exemption/

In recent years, the Conservative government has sought to make amendments to GDPR in the UK, through the Data Protection and Digital Information Bill.[152] In March 2024, an open letter from civil society groups, including Liberty, Public Law Project, Connected by Data and several unions, also argued that in order to increase transparency around the use of automated decision making (ADM) in the public sector, the Algorithmic Transparency Recording Standard should be made mandatory.[153] The authors argue that this step will ensure that individuals are able to seek redress when systems fail or operate unlawfully.[154]

Following the 2024 General Election in July, the new Labour government has introduced a similar bill to the Conservative's Data Protection and Digital Information Bill, called the Data Use and Access Bill.[155] The stated goals of the Data Use and Access Bill are economic growth, increased efficiency and improved public services.[156] At the time of writing, critics are concerned that the bill will undermine digital rights, such as by reforming the legal framework governing Automated Decision Making (Clause 80), and expanding law enforcement and other exemptions (Clauses 124-126; Clause 70).

CS 1.2 Global approaches to data privacy

Two major global frameworks have emerged that establish important principles and obligations regarding data privacy: the Global Digital Compact (GDC) and the Council of Europe AI Treaty. These frameworks demonstrate growing international consensus around data privacy protections while highlighting remaining challenges in global governance.

The Global Digital Compact establishes data privacy as a core component of digital rights. This is evident in objective 4 that aims to: 'Advance responsible, equitable and interoperable data governance approaches and legitimate purposes, in compliance with international law (all SDGs)'.[157] Key provisions include:

- ***Article 39b:*** *Strengthen support to all countries to develop effective and interoperable national data governance frameworks (all SDGs);*[158]
- ***Article 39c:*** *Empower individuals and groups with the ability to consider, give and withdraw their consent to the use of their data and the ability to choose how those data are used, including through legally mandated protections for data privacy and intellectual property (SDGs 10 and 16);*[159]
- ***Article 39d:*** *Ensure that data collection, access, sharing, transfer, storage and processing practices are safe, secure and proportionate for necessary, explicit and legitimate purposes, in compliance with international law (all SDGs).*[160]

152 TechUK (2024) "The Data (Use and Access) Bill: What's changed and what remains from the DPDI Bill". https://www.techuk.org/resource/the-data-use-and-access-bill-what-s-changed-and-what-remains-from-the-dpdi-bill.html.
153 Public Law Project, The Algorithmic Transparency Recording Standard and the need for a statutory duty (2024). https://publiclawproject.org.uk/content/uploads/2024/03/ATRS-joint-letter.pdf
154 Ibid.
155 Department for Science, Innovation and Technology, the Department of Health and Social Care, the Home Office, the Department for Business and Trade, HM Treasury and the Department for Energy Security and Net Zero (2024) "Data (Use and Access) Bill". https://bills.parliament.uk/publications/56527/documents/5211
156 Department for Science, Innovation and Technology (2024) "New data laws unveiled to improve public services and boost UK economy by £10 billion". https://www.gov.uk/government/news/new-data-laws-unveiled-to-improve-public-services-and-boost-uk-economy-by-10-billion
157 United Nations (2024) Global Digital Compact, Objective 4.
158 United Nations (2024) Global Digital Compact, Art 39b.
159 United Nations (2024) Global Digital Compact, Art 39c.
160 United Nations (2024) Global Digital Compact, Art 39d.

The Council of Europe's AI Treaty reinforces strong privacy safeguards, building on global standards.[161]

- ***Article 11:*** *Each Party shall adopt or maintain measures to ensure that, with regard to activities within the lifecycle of artificial intelligence systems:*
  - ***Article 11a:*** *privacy rights of individuals and their personal data are protected, including through applicable domestic and international laws, standards and frameworks;*[162] *and*
  - ***Article 11b:*** *effective guarantees and safeguards have been put in place for individuals, in accordance with applicable domestic and international legal obligations.*[163]

Both frameworks offer robust privacy protections, but differ in enforceability. The GDC provides guiding principles for universal privacy standards, while the Council of Europe Treaty establishes binding commitments for its parties, enhancing accountability. However, the voluntary nature of the GDC may limit its impact compared to the treaty's formal mechanisms.

APPROACHES TO DATA PRIVACY BY THE GOVERNMENT OF THE REPUBLIC OF SOUTH KOREA

In South Korea, privacy is included in its Digital Bill of Rights, namely:[164]

- *Article 9 Access and Control of Personal Information: Every individual shall be able to access and control their personal information in the digital environment, including requesting access to, correction, deletion, and transfer of such information.*
- *Article 19 Protection of Digital Privacy: In the digital environment, the privacy of individuals shall be protected from unlawful identification and tracking, including digital surveillance and location tracking.*

In its policy actions, the Government of the Republic of Korea government already requires its public institutions to register and disclose information about personal information files (personal information portal, www.privacy.go.kr) and supports information subjects to request information access, correction, deletion, and suspension of processing.[165] Since 2022, it has also been developing personal information protection enhancement technology and published the "Guidelines on Biometric Information Protection" which define the basic principles and protective measures for each processing stage for the safe use of biometric information such as fingerprints and iris.

161 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series. http://rm.coe.int/1680afae3c
162 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Article 11a.
163 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 11b.
164 The Government of the Republic of Korea (2023) "South Korean Digital Bill of Rights". https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=
165 The Government of the Republic of Korea (2023) "Digital Bill of Rights commentary: Results of the 2023 Diagnosis of Response to Digital Deepening". Available on request.

CASE STUDY 2
BALANCING FREEDOM OF EXPRESSION WITH ONLINE SAFETY IN DIGITAL ENVIRONMENTS

As indicated in Chapter 3, the global power and reach of social media platforms, combined with a number of significant concerns and allegations of influence in elections, suicides and genocides, have caused governments in Europe and the UK to strengthen digital rights protections in the online digital environment. There has been particular concern surrounding balancing the rights to freedom of expression, protection from discrimination as well as childrens' safety.

CS 2.1 European approaches

In the Declaration of Digital Rights and Principles, the EU also aims to achieve protections for a range of digital rights, spanning freedom of expression in the digital environment, facilitating free democratic debate as well as ensuring children are protected and empowered in the digital environment, for example:[166]

- ***Article 13:*** *Everyone has the right to freedom of expression and information, as well as freedom of assembly and of association in the digital environment.*
- ***Article 15:*** *Online platforms, particularly very large online platforms, should support free democratic debate online. Given the role of their services in shaping public opinion and discourse, very large online platforms should mitigate the risks stemming from the functioning and use of their services, including in relation to misinformation and disinformation campaigns, and protect freedom of expression.*
- ***Article 20:*** *Children and young people should be empowered to make safe and informed choices and express their creativity in the digital environment.*
- ***Article 21:*** *Age-appropriate materials and services should improve experiences, well-being and participation of children and young people in the digital environment.*

The Digital Services Act

One such policy approach that contributes to the right to freedom of expression online as well as the protection and empowerment of children that has already been developed and launched in the EU is the Digital Services Act. This is analysed through a digital rights lens below.[167]

166 European Declaration on Digital Rights and Principles (2022) https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles
167 European Commission (2022) Digital Services Act https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

In 2022, the European Commission passed the Digital Services Act (DSA), a set of rules designed to govern digital services that serve as intermediaries for consumers, goods, services and content, such as host providers, online marketplaces and social media networks.[168] The DSA was introduced alongside the Digital Markets Act (DMA), with the latter focusing on the regulation of the market.

The Act builds upon the 2000 e-Commerce Directive to address the new challenges and realities of the digital world, particularly those posed by Very Large Online Platforms (VLOPs) and Very Large Search Engines (VLOSEs).[169] The central aim of the DSA is to prevent illegal and harmful activities online including the spread of disinformation. It does so primarily by expanding the rights of users and the transparency obligations of service providers. As of February 2024, the DSA became fully applicable throughout the EU. The enforcement of the Digital Services Act is to be a coordinated effort between the Commission and the national authorities.

Overall, the Act has been praised for the protections it provides not just for freedom of expression, but also non-discrimination. However, the Act has received some criticism with concerns that approaches such as trusted flaggers (discussed further below), watermarking and the notice and take down mechanism actually undermine the protection of freedom of expression. In addition, there are concerns that the absence of explicit privacy protections undermines other rights to privacy such as user autonomy over personal data and risks discrimination.

168 https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers
169 https://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive

The following Table 2 captures the strengths and weaknesses of the Act in greater detail through the lens of digital rights. Enabling factors such as transparency, enforcement and remedy are used to colour code these when relevant.

TABLE 2
STRENGTHS AND WEAKNESSES OF THE DIGITAL SERVICES ACT IN THE EU THROUGH THE LENS OF DIGITAL RIGHTS

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Freedom of expression and information	The DSA reinforces an EU-wide ban on active fact-finding obligations and general content monitoring so platforms are not required to systematically police content in a way that harms free speech.[170] The DSA retains conditional immunity for hosting providers which protects against arbitrary removals of content. The maintenance of this conditional immunity has been described by some as 'the cornerstone of freedom of expression.'[171] The DSA obligates platforms to provide a statement of reasons to users that have been blocked, removed, or demoted.[172] The DSA has expanded user redress so people can tackle decisions to block, remove, or demote made by VLOPs. The Act has provided a three-tiered grievance mechanism: internal complaint handling system provided by platforms free of charge, out of court dispute settlement and judicial redress.[173]	DSA regulations encourage the adoption of watermarking on generative AI content to counter disinformation. However, some evidence suggests that watermarking does not adequately counter disinformation and instead poses a risk to freedom of expression and privacy.[174] The Act outlines a notice and takedown mechanism to counter illegal and harmful content. However, this mechanism has been criticised for giving hosting providers unilateral power and for facilitating the over removal of legal content. Notice and takedown dictates the inability to urgently remove or disable access to illegal content may lead to loss of immunity from liability, enforcement may be over-excessive and at odds with freedom of expression.[175] The Act prioritises actioning notices from trusted flaggers on illegal and harmful content. Trusted flaggers are special, EU-based entities that must meet three criteria: (a) Expertise and competence, (b) Independence and (c) Diligence, accuracy and objectivity. Yet, because law enforcement could be appointed trusted flaggers, some have pointed out that there is a risk of enforcement overreach.[176]

170 Algorithm Watch. A guide to the Digital Services Act, the EU's new law to rein in Big Tech. 2022. https://algorithmwatch.org/en/dsa-explained/; Article 19. EU: Will the Digital Services Act hold Big Tech to account. 2022. https://www.article19.org/resources/digital-services-act-big-tech-accountable/
171 Ibid
172 Algorithm Watch. A guide to the Digital Services Act, the EU's new law to rein in Big Tech. 2022. https://algorithmwatch.org/en/dsa-explained/
173 Pirkova, E. The Digital Services Act: your guide to the EU's new content moderation rules. Access Now, 2022. https://www.accessnow.org/digital-services-act-eu-content-moderation-rules-guide/
174 Article 19. EU: Platforms' election risk mitigation measures must put human rights first. 2024. https://www.article19.org/resources/eu-platforms-election-risk-mitigation-measures-must-put-rights-first/
175 Ibid
176 Ibid; European Commission. Trusted flaggers under the Digital Services Act (DSA). https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa; EDRi and Hate Aid (2023) "How to protect fundamental rights when appointing trusted flaggers" https://edri.org/wp-content/uploads/2023/12/Trusted-Flaggers-guide-for-designation.pdf

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Freedom of expression and information		Enforcement of the Act requires a coordinated effort between the Commission and Member States. However, there are concerns that this is leading to an overly broad implementation of the DSA, as can be seen in the 'Securiser et reguler l'espace numerique' bill in France.[177] Concepts of 'hate speech,' Foreign Information Manipulation and Interference (FIMI), or 'disinformation' are repeatedly used yet not clearly defined. As such, the definitions are ill-suited to base restrictions of expressions on.[178] The DSA outlines a crisis response mechanism. This gives the European Commission the ability to control the freedom of expression on large online platforms when it decides a crisis has taken place. This could hinder freedom of expression as well as restrict access to information. The DSA does not seek to decentralise content curation or open the market to alternative players. VLOPs are not obligated to unbundle hosting from content curation nor allow third parties to provide alternative recommendation systems despite knowledge that recommendation algorithms promote extreme and controversial speech at the expense of other voices. As such, the DSA fails to offer real information diversity.
Freedom of thought, conscience and religion		The DSA does not substantially tackle the business model of platforms that are based on behavioural advertising. As such, despite some restrictions on online manipulation, the Act does not tackle the fundamental basis of platforms that infringe upon the freedom of thought via manipulation.[179]

177 Article 19. EU: Digital Services Act does not provide green light for platform blocking. 2023. https://www.article19.org/resources/eu-dsa-does-not-provide-a-green-light-for-platform-blocking/
178 Article 19. EU: Platforms' election risk mitigation measures must put human rights first. 2024. https://www.article19.org/resources/eu-platforms-election-risk-mitigation-measures-must-put-rights-first/
179 Article 19. EU: Will the Digital Services Act hold Big Tech to account. 2022. https://www.article19.org/resources/digital-services-act-big-tech-accountable/

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Non-discrimination	DSA requires VLOPs and VLOSEs to carry out annual risk assessments. These assessments must include a broad list of systemic risks. This supports the mitigation of the wide range of potential adverse impacts.[180] The DSA has established a ban on profiling individuals based on 'sensitive' traits such as religion or sexuality.[181] Platforms will be required to share internal data with auditors, EU, Member State authorities and researchers from academia and civil society to facilitate scrutiny and accountability.[182]	
Privacy	The Act has strengthened user's right to online anonymity and private communication. The Act has also explained that users should have the right to use and pay for services anonymously wherever reasonable.[183]	The Act does not offer an explicit right for users to have encryption and anonymity.[184] The Act allows the government to uncover data about anonymous speakers and others without having to face adequate procedural safeguards.[185] The notice and takedown mechanism takes down user communication which is likely to interfere with the right to privacy.[186]

180 Algorithm Watch. A guide to the Digital Services Act, the EU's new law to rein in Big Tech. 2022. https://algorithmwatch.org/en/dsa-explained/; Amnesty International. What the EU's Digital Services Act means for human rights and harmful Big Tech business models. 2022. https://www.amnesty.org/en/documents/pol30/5830/2022/en/
181 Algorithm Watch. (2022) A guide to the Digital Services Act, the EU's new law to rein in Big Tech. https://algorithmwatch.org/en/dsa-explained/
182 Ibid
183 Komaitis, K., Rodriguez, K. and Schmon C. (2022) Enforcement Overreach Could Turn Out To Be A Real Problem in the EU's Digital Services Act. Electronic Frontier Foundation https://www.eff.org/deeplinks/2022/02/enforcement-overreach-could-turn-out-be-real-problem-eus-digital-services-act
184 Article 19. (2022) EU: Will the Digital Services Act hold Big Tech to account. https://www.article19.org/resources/digital-services-act-big-tech-accountable/
185 Komaitis, K., Rodriguez, K. and Schmon C. (2022) Enforcement Overreach Could Turn Out To Be A Real Problem in the EU's Digital Services Act. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2022/02/enforcement-overreach-could-turn-out-be-real-problem-eus-digital-services-act
186 Ibid

UK approaches

The Online Safety Act (OSA) is a new regulatory framework for national online governance, brought into law by the United Kingdom in 2023. The Act seeks to protect adults and children by increasing the obligations on social media companies and search engines (henceforth described as 'platforms') to ensure user safety on their respective platforms.[187]

The OSA has five policy objectives, some of which relate to digital rights. These include increasing user safety, preserving and enhancing freedom of speech online, improving the ability of law enforcement to tackle illegal content online, improving user ability to keep themselves safe, and improving society's understanding of the harm landscape.[188] The Act categorises platforms into three groups according to level of risk and requires additional obligations for the riskiest.[189]

The OSA expands the powers of Ofcom to be the independent regulator of the Act. The body is responsible to both set out guidance and to then assess and enforce compliance. The Act will require secondary legislation to enforce certain parts of the framework.[190] The Act has introduced a number of criminal offences: encouraging or assisting self harm, cyberflashing, sending false information to cause non-trivial harm, threatening communications, intimate image abuse and epilepsy trolling.

Prior to becoming legislation, the Online Safety Bill was divisive in itself and sparked debate around the rights of internet users in the UK and globally. This debate was reflected in the progress and development of the Bill. In light of the 2024 August riots, and while Ofcom's duties and codes remain under consultation (and therefore non-operational), the OSA has faced renewed critique for not doing enough to tackle the spread of mis/disinformation.[191]

Overall, the Act has received very mixed reviews from digital rights organisations. Some have praised the act for the new protections it provides particularly from children's rights organisations. However, it has also received fierce criticism for the risks certain protections for safety represent to other rights such as privacy and free expression particularly in relation to the implications for the weakening of end-to-end encryption.

The following Table 3 captures the strengths and weaknesses of the Act in much more detail through the lens of digital rights. Enabling factors such as transparency, enforcement and remedy are used to colour code these when relevant.

187 DSIT. (2024) Online Safety Act: explainer. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#what-the-online-safety-act-does

188 Woodhouse, J. (2022) Online Safety Bill: Progress of the Bill. House of Commons Library: Research Briefing. https://researchbriefings.files.parliament.uk/documents/CBP-9579/CBP-9579.pdf

189 Woods, L. and Walsh, M. (2024) Categorisation of services in the Online Safety Act. Online Safety Act Network. https://www.onlinesafetyact.net/analysis/categorisation-of-services-in-the-online-safety-act/

190 DSIT. (2024) Online Safety Act: explainer. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#what-the-online-safety-act-does

191 Woods, L., Antoniou, A., (2024) "Is the Online Safety Act 'fit for purpose'". https://blogs.lse.ac.uk/medialse/2024/09/03/is-the-online-safety-act-fit-for-purpose/ ; Full Fact. (2024) The Online Safety Act and Misinformation: What you need to know. https://fullfact.org/policy/online-safety-act/

TABLE 3
STRENGTHS AND WEAKNESSES OF THE ONLINE SAFETY ACT IN THE UK THROUGH THE LENS OF DIGITAL RIGHTS

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Children's rights	The OSA requires proper enforcement of age limits. This will require platforms to prevent children from accessing harmful or age-inappropriate content such as pornography, serious violence, bullying, self harm and eating disorders.[192] Platforms must declare what tools they are using and must demonstrate how they enforce their age limits.[193] All platforms, regardless of size, are required to carry out risk assessments. This could allow for more targeted content moderation and greater harm mitigation.[194] Platforms that are likely to be accessed by children have to take action to protect children against content that poses a material risk of causing significant physical or psychological impact.[195] Larger platforms must publish a summary of their risk assessments to be transparent about potential harms to children.[196] The OSA enforces higher financial penalties (maximum of £18m or 10% of qualifying worldwide revenue) and imprisonment of senior management (maximum of up to 2 years) in serious cases of non-compliance with specific child safety duties or in respect of child abuse and exploitation.[197]	Whilst the OSA requires platforms to allow users and affected persons to report content they view as illegal or harmful to children, as the OSA has no independent complaints mechanism, services have discretion in how they address investigations of reported content.[198] User reporting mechanisms for content harmful to children risks placing an unproportionate burden on children/ victims of abuse to take action.[199] Depending on how it's implemented, age assurance could risk a number of other digital rights. Using card details for age verification risks social discrimination against those without a payment card. Facial age estimation using biometric data risks privacy with threats such as video capture and possible blackmail.[200] (See privacy and freedom of expression)

192 NSPCC Learning. The Online Safety Act: what it means for children and professionals. 2023. https://learning.nspcc.org.uk/news/2023/november/what-online-safety-act-means-children-professionals
193 DSIT and Home Office. The Online Safety Act Impact Assessment. 2024. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf; NSPCC Learning. The Online Safety Act: what it means for children and professionals. (2023) https://learning.nspcc.org.uk/news/2023/november/what-online-safety-act-means-children-professionals
194 NSPCC Learning. (2023) The Online Safety Act: what it means for children and professionals. https://learning.nspcc.org.uk/news/2023/november/what-online-safety-act-means-children-professionals
195 DSIT and Home Office. (2024) The Online Safety Act Impact Assessment. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf
196 NSPCC Learning. (2023) The Online Safety Act: what it means for children and professionals. https://learning.nspcc.org.uk/news/2023/november/what-online-safety-act-means-children-professionals
197 Fieldfisher and 5 Rights Foundation. (2023) The Online Safety Act: A comparative legal analysis of the provisions for children. https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights-fieldfisher-legal-analysis-osa-final.pdf
198 5Rights Foundation. The Online Safety Act: A comparative legal analysis of the provisions for the children. 2023. https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights-fieldfisher-legal-analysis-osa-final.pdf
199 VAWG. VAWG Sector Experts Response To Ofcom's Protection of Children's Consultation. 2024. https://www.onlinesafetyact.net/uploads/vawg-response-july-2024-ofcom-s-protection-of-children-consultation.pdf
200 Commission Nationale Informatique & Libertes. Online age verification: balancing privacy and the protection of minors. 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors; Open Rights Group. UK Online Safety Bill Will Mandate Dangerous Age Verification For Much Of The Web. 2023. https://www.openrightsgroup.org/publications/uk-online-safety-bill-will-mandate-dangerous-age-verification-for-much-of-the-web/

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Privacy	The OSA maintains the right to anonymity. It requires platforms to offer optional user verification.[201] The OSA places explicit duty on providers to carry out privacy impact assessments.[202]	Ofcom can issue notices to platforms service providers to proactively take down illegal content e.g. Child Sexual Abuse Material (CSAM). However, doing so may require breaking end-to-end encryption or enable 'client-side scanning' which threatens privacy and security. Privacy rights groups regard this approach as disproportionate government interference and surveillance.[203] The age assurance requirements in the OSA have the potential to use personal data.[204]
Freedom of expression and information	The OSA will require all platforms to have user reporting mechanisms. This is to enable harmful content to be flagged and removed and further harm to potential viewers is prevented.[205] The OSA requires Category 1 platforms to ensure they have clear and accessible terms of service as well as user redress mechanisms. This will require Category 1 platforms to balance content moderation powers with the consideration of freedom of expression: they now have to be clear on acceptable content, enforce rules consistently and provide users effective mechanisms for remedy.[206]	The OSA provides protections for news publisher content and journalistic content which may offer some people (and those commenting beneath news articles posted on social media) with a higher level of protection. For example, newspapers and broadcasters will be given special notice before their content is moderated, or receive expedited complaints procedures for platform action related to such journalistic content.[207]

201 Department for Science, Innovation and Technology and Home Office. The Online Safety Act Impact Assessment. 2024. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf
202 DSIT and Home Office. The Online Safety Act Impact Assessment. 2024. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf
203 Dewsnip, K. The Online Safety Act: scrutiny, safeguards and civil liberties. The Constitution Society, 2023. https://consoc.org.uk/the-online-saftey-act/#:~:text=Conversely%2C%20not%20all%20of%20the,the%20newly%20created%20criminal%20offences); Index on Censorship. Our manifesto: the next UK government's necessary actions to restore freedom of expression. 2024. https://www.indexoncensorship.org/2024/06/our-manifesto-the-next-uk-governments-necessary-actions-to-restore-freedom-of-expression/; Glitch. What will the Online Safety Act mean for Black women? 2023. https://glitchcharity.co.uk/what-will-the-online-safety-act-mean-for-black-women/; Article 19 (2024) "New government must prioritise freedom of expression". https://www.article19.org/resources/uk-new-government-must-prioritise-freedom-of-expression/
204 Commission Nationale Informatique & Libertes. Online age verification: balancing privacy and the protection of minors. 2022. https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors
205 DSIT and Home Office. The Online Safety Act Impact Assessment. 2024. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf
206 DSIT and Home Office. The Online Safety Act Impact Assessment. 2024. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf
207 DSIT and Home Office. The Online Safety Act Impact Assessment. 2024. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf; Hern, A. What is the UK's Online Safety Act and what powers will it provide? The Guardian, 2024. https://www.theguardian.com/law/article/2024/aug/08/what-is-uk-online-safety-act-new-legislation-laws; Judson, E. The Online Safety Bill, Demos Position Paper. Demos, 2022. https://demos.co.uk/wp-content/uploads/2023/02/OSB-position-paper.pdf

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Freedom of expression and information	The protections offered for journalistic content focuses on the content but not the actor. This is to ensure quality democratic debate by protecting journalists across the spectrum as well as to protect the public's access to journalism. The Act creates the Upper Tribunal which allows appeals from platforms or other people with sufficient interest against the decisions made by Ofcom.[208] The OSA requires platforms to offer users tools through which they can filter out content from non-verified users, and prevent non-verified users from interacting with their content. Consequently, the OSA will empower users to determine the content and users they interact with.[209] The OSA expands upon the Ofcom existing statutory duty to promote media literacy in relation to social media and search platforms, under the 2003 Communications Act.[210] The inclusion of media literacy in the Act supports digital citizenship and is an important step towards preventing online abusive behaviour, particularly towards those disproportionately targeted, such as Black women.[211]	Enforcement of the OSA is criticised for being heavily reliant on secondary legislation and non-statutory guidance. Particular concern has been expressed over the reliance on Ofcom to regulate and enforce the regime, particularly as it is an unelected body.[212] The OSA has created a new 'false communications offence.' This is sending knowingly false communications to intentionally cause non-trivial emotional, physical or psychological harm. Whilst critics accept this offence may work in some specific cases, they display concern about how this vague definition may work at internet scale. It has been suggested such a definition could risk inappropriate takedown of content.[213]

208 Department for Science, Innovation and Technology and Home Office. (2024) The Online Safety Act Impact Assessment. https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf; The National Archives. (2023) The Online Safety Act. Open Government License, 2023. https://www.legislation.gov.uk/ukpga/2023/50/part/8/chapter/1#:~:text=168Appeals%20against%20OFCOM%20noticesU.K.&text=may%20be%20brought%20by%20any,leave)%20of%20the%20Upper%20Tribunal.

209 Department for Science, Innovation and Technology and Home Office. (2024) The Online Safety Act Impact Assessment: https://assets.publishing.service.gov.uk/media/6716222b9242eecc6c849b09/Online_Safety_act_enactment_impact_assessment.pdf

210 Ibid

211 Glitch. (2023) What will the Online Safety Act mean for Black women? 2023.https://glitchcharity.co.uk/what-will-the-online-safety-act-mean-for-black-women/

212 Dewsnip, K. (2023) The Online Safety Act: scrutiny, safeguards and civil liberties. The Constitution Society. https://consoc.org.uk/the-online-saftey-act/#:~:text=Conversely%2C%20not%20all%20of%20the,the%20newly%20created%20criminal%20offences

213 Full Fact. (2024) The Online Safety Act and Misinformation: What you need to know. https://fullfact.org/policy/online-safety-act/

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Freedom of expression and information		Ofcom has so far failed to provide meaningful guidance on how to balance accurate content removal with speedy takedowns. This exacerbates the existing risk for the wrongful takedown of legal content produced by already marginalised or vulnerable groups such as activists, racialised and/ or queer communities, migrant communities posting in non-Western languages.[214] Protections from health misinformation, misinformation during 'information incidents', and election disinformation were also not included in the final version of the OSA.[215] The OSA also lacks regulatory oversight for what platforms include in their terms of services regarding what content is not allowed on their platforms which means it will neither prevent misinformation from spreading, nor protect freedom of expression.[216]
Freedom of thought, conscience and religion		Small but illegal and harmful forums based abroad may be beyond the reach of Ofcom. The BBC outlines an online suicide room that remains active and accessible even following the OSA.[217]

214 Burke, A. (2024) A Dangerous Precedent for Global Censorship. Open Rights Group: https://www.openrightsgroup.org/blog/a-dangerous-precedent-for-global-censorship/
215 Full Fact. The Online Safety Act and Misinformation: What you need to know. https://fullfact.org/policy/online-safety-act/
216 Ibid
217 Crawford, A. (2024) The Online Safety Act is one year old. Has it made children any safer. BBC News https://www.bbc.co.uk/news/articles/c5y38z4pk9lo

DIGITAL RIGHT	STRENGTHS	WEAKNESSES
Non-discrimination	The Act clearly prohibits posts that spread hate speech, as well as posts that target or harass individuals or groups based on race, religion, religion or other protected characteristics. Platforms are required to take swift actions against cases of hate speech.[218] The Act's creation of new offences and the provision of related Ofcom guidance crucially delivers greater protections for women and girls, who are affected disproportionately by online harms.[219] These offences include the sending of threatening communications, such as rape threats, sending sexually graphic images to intentionally cause alarm, distress and/ or humiliation and threatening and/ or sharing intimate photographs without the consent to cause alarm, distress and/ or humiliation.[220]	The Act and Ofcom guidance does not go far enough in protecting people from multiply-marginalised communities.[221] The Act's weakening of end-to-end encryption for service providers particularly risks critical threats to marginalised or vulnerable communities such the LGBTQIA+ community, journalists and victims of domestic abuse. Additionally, the case of Podchasov v. Russia, the ECHR clarified that the removal or limitation of encryption to target criminals is not proportionate.[222] Categorisation of the risk platforms pose on the basis of user number and functionalities may exclude smaller platforms that house extremist content from the additional obligations required of those classed as Category 1.[223]

218 Lawdit Solicitors. (2024) What is the Online Safety Act 2024? https://lawdit.co.uk/readingroom/what-is-the-online-safety-act-2024
219 Woods, L. Perrin, W. and Walsh, M. (2023) It's (nearly) here: a short guide to the Online Safety Act. Carnegie UK https://carnegieuktrust.org.uk/blog-posts/its-nearly-here-a-short-guide-to-the-online-safety-act/
220 Brett Wilson LLP. (2024) The Online Safety Act 2023: nine new criminal offences come into force https://www.brettwilson.co.uk/blog/the-online-safety-act-2023-nine-new-criminal-offences-come-into-force/
221 Glitch (2024) The Online Safety Act is only one step towards ending online abuse - and its effective enforcement is vital. https://glitchcharity.co.uk/online-safety-act/
222 Burke, A. (2024) A Dangerous Precedent for Global Censorship. Open Rights Group. https://www.openrightsgroup.org/blog/a-dangerous-precedent-for-global-censorship/
223 Antisemitism Policy Trust. The Online Safety Bill: House of Lords Stages. https://antisemitism.org.uk/resource/online-safety-bill-lords-stages/

CS 2.2 Global approaches to balancing different digital rights in online environments such as social media platforms

Both the GDC and the Council of Europe Treaty address digital rights in online environments, particularly by focusing on content moderation, platform responsibility, and freedom of expression. The Global Digital Compact establishes comprehensive provisions regarding online safety and freedom of expression. For example, under Objective 3, it mandates that parties must "foster an inclusive, open, safe and secure digital space that respects, protects and promotes human rights."

Specifically on content moderation and platform responsibilities, the GDC states:

- ***Article 32c:*** *Call on digital technology companies and social media platforms to provide online safety-related training materials and safeguards to their users, and in particular, related to children and youth users (SDG 3).*[224]
- ***Article 32d:*** *Call on social media platforms to establish safe, secure and accessible reporting mechanisms for users and their advocates to report potential policy violations, including special reporting mechanisms adapted to children and persons with disabilities (SDG 3).*[225]

On information integrity and freedom of expression, the GDC requires parties to:

- ***Article 35b:*** *Promote diverse and resilient information ecosystems, including by strengthening independent and public media and supporting journalists and media workers.*[226]
- ***Article 35c:*** *Provide, promote and facilitate access to and dissemination of independent, fact-based, timely, targeted, clear, accessible, multilingual and science-based information to counter misinformation and disinformation.*[227]

The Council of Europe AI Treaty complements these provisions through Article 5 which requires parties to:

- ***Article 5(1):*** *adopt or maintain measures that seek to ensure that artificial intelligence systems are not used to undermine the integrity, independence and effectiveness of democratic institutions and processes.*[228]
- ***Article 5(2):*** *protect its democratic processes in the context of activities within the lifecycle of artificial intelligence systems, including individuals' fair access to and participation in public debate, as well as their ability to freely form opinions.*[229]

224 United Nations (2024) Global Digital Compact, Art 32c.
225 United Nations (2024) Global Digital Compact, Art 32d.
226 United Nations (2024) Global Digital Compact, Art 35b.
227 United Nations (2024) Global Digital Compact, Art 35b.
228 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 5(1).
229 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 5(2) .

APPROACHES TO DIGITAL RIGHTS PROTECTIONS IN DIGITAL ENVIRONMENTS LIKE SOCIAL MEDIA PLATFORMS BY THE GOVERNMENT OF THE REPUBLIC OF SOUTH KOREA

South Korea's Digital Bill of Rights mirrors this trend of protections by establishing an explicit, be it qualified, protection for the freedom of expression in digital environments:[230]

- ***Article 7 Freedom of Digital Expression:*** *Every individual shall be able to freely express their views in the digital environment; provided, however, that such expression shall be carried out responsibility so as not to infringe upon the honor and rights of others, public morality, or social ethics.*

In their policy actions, the Government of the Republic of South Korea has focused on ensuring citizens can discern good quality information.[231] It has established twelve viewer media centres across the country to promote customised 'false information capacity-building' training for different target groups e.g. young people, adults, seniors. This includes introducing case studies of the damage done by false information and practical classes on article writing, with the aim of equipping people with the ability to discern the authenticity of information and utilise it properly.

230 The Government of the Republic of Korea. (2023) South Korean Digital Bill of Rights. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=

231 The Government of the Republic of Korea. (2023) South Korean Digital Bill of Rights. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=

CASE STUDY 3
HUMAN-CENTRIC TECHNOLOGICAL DEVELOPMENT

Building on the broad protections for user rights in digital environments, policymakers have also grappled with regulating specific digital technologies, such as Artificial Intelligence.

CS 3.1 European approaches

The European Declaration of Digital Rights and Principles prescribes for a conscientious and person-centric approach to technological development:[232]

- ***Article 9:*** *Everyone should be empowered to benefit from the advantages of algorithmic and artificial intelligence systems including by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights.*

The development of the EU's Artificial Intelligence Act is an example of the EU's approach to enacting this principle. It's the world's first comprehensive legislation on AI and was brought into law in 2024 by the European Union.[233]

The AI Act categorises AI systems into four different risk classification. Those deemed to pose an unacceptable risk are now entirely banned for deployment and use in the EU, except for law enforcement . These include those based on cognitive behavioural manipulation, particularly for vulnerable groups such as children, social scoring, biometric identification and categorisation as well as real time and remote biometric identification.[234] Those considered high risk must comply with the most stringent of conditions, such as expanded transparency requirements. Finally, those considered limited and minimal risk are largely left unregulated.

Overall, the Act has been praised for its protections to children's rights and freedom of expression and information. It pays particular attention to the threats posed by AI to children and seeks to circumvent these by banning systems considered unacceptably dangerous and mandating strict risk management processes. It also protects the freedom of expression through detailed user redress mechanisms that aim to hold major platforms accountable. Similarly, the requirement to register the use of high-risk AI systems alongside fundamental rights impact assessments holds AI system deployers to account and helps mitigate against the risk of discrimination. However, critics assert that the Act does not go far enough in its transparency and accessibility requirements. By limiting transparency requirements to public sector deployers, the Act prevents private deployers and law enforcement officers from adequate scrutiny. This prevents adequate protection against discrimination and invasions of privacy.

232 European Declaration on Digital Rights and Principles (2022) https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles
233 European Parliament. EU AI Act: first regulation on artificial intelligence. 2023. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
234 European Parliament. EU AI Act: first regulation on artificial intelligence. 2023. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

The following Table 4 captures the strengths and weaknesses of the Act through the lens of digital rights. Enabling factors such as transparency, enforcement and remedy are used to colour code these when relevant.

TABLE 4
STRENGTHS AND WEAKNESSES OF THE EU'S AI ACT THROUGH THE LENS OF DIGITAL RIGHTS

DIGITAL RIGHT	STRENGTH	WEAKNESS
Children's rights	The Act bans AI systems that are based on the exploitation of age vulnerabilities. For example, AI toys that can encourage dangerous behaviour.[235] High risk AI systems, such as those used in education, must take special account of children and their rights in their risk management processes.[236] Some children's rights groups suggest watermarking is an important way to protect children when they are interacting with deep fake and generative AI systems.[237]	Children's rights critics argue that the Act pays insufficient attention to the specific vulnerabilities children face with deep fake and generative AI.[238]
Equality of human rights		The AI Act fails to adequately protect the rights of people that reside outside the European Union. This is because AI systems that have been classified as unacceptable can be exported outside of the EU.[239]

235 EU Team. European Parliament's revisions of AI Act risk jeopardising child safety. 5 Rights Foundation, 2023. https://5rightsfoundation.com/european-parliaments-revisions-of-ai-act-risk-jeopardising-child-safety/; Kurian, N. EU AI Act: How Well Does It Protect Children and Young People. Leverhulme Centre For The Future Of Intelligence., 2024. https://www.lcfi.ac.uk/news-events/blog/post/eu-ai-act-how-well-does-it-protect-children-and-young-people.
236 EU Team. European Parliament's revisions of AI Act risk jeopardising child safety. 5 Rights Foundation, 2023. https://5rightsfoundation.com/european-parliaments-revisions-of-ai-act-risk-jeopardising-child-safety/; Kurian, N. EU AI Act: How Well Does It Protect Children and Young People. Leverhulme Centre For The Future Of Intelligence., 2024. https://www.lcfi.ac.uk/news-events/blog/post/eu-ai-act-how-well-does-it-protect-children-and-young-people.
237 EU Team. European Parliament's revisions of AI Act risk jeopardising child safety. 5 Rights Foundation, 2023. https://5rightsfoundation.com/european-parliaments-revisions-of-ai-act-risk-jeopardising-child-safety/
238 Kurian, N. EU AI Act: How Well Does It Protect Children and Young People. Leverhulme Centre For The Future Of Intelligence., 2024. https://www.lcfi.ac.uk/news-events/blog/post/eu-ai-act-how-well-does-it-protect-children-and-young-people.
239 Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf

DIGITAL RIGHT	STRENGTH	WEAKNESS
Equality of human rights		The AI Act develops a separate legal framework for migration control authorities. This enables the testing and disproportionate use of dangerous surveillance technologies at borders.[240] Non-remote biometric identification systems, fingerprint scanners, forecasting tools can be used to predict, interdict and curtail migration.[241]
Freedom of expression and information	The Act requires providers and (public use) deployers of high risk AI systems to register their use in a publicly accessible EU database. For providers, this must be with a statement on the intended purpose of the system, the information used and its operating logic. For public authority deployers, this must be with a summary of the findings from the fundamental rights impact assessment and the data protection impact assessment.[242] The Act lays out means for redress for people that have been affected by AI systems. They will have a right to an explanation and will be able to issue a complaint.[243]	Law enforcement and migration officials only have to register a limited amount of information about their use of high risk systems that is kept outside of public view. This prevents groups such as affected parties and bodies such as civil society organisations from holding these bodies accountable in high-stake areas.[244] Private users of high risk AI systems do not have to register their use which limits scrutiny and accountability.[245]

240 Rodelli, C. The EU AI Act: How to (truly) protect people on the move. Access now, 2023. https://www.accessnow.org/eu-ai-act-migration/; Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf.
241 Rodelli, C. The EU AI Act: How to (truly) protect people on the move. Access now, 2023. https://www.accessnow.org/eu-ai-act-migration/; Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf
242 Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf
243 European Centre for Not-for-Profit Law. Big Win for Fundamental Rights, As The European Parliament Adopts The AI Act. 2023. https://ecnl.org/news/big-win-fundamental-rights-european-parliament-adopts-ai-act; Muller, A. and Spielkamp, M. AI Act deal: Key safeguards and dangerous loopholes. Algorithm Watch, 2023. https://algorithmwatch.org/en/ai-act-deal-key-safeguards-and-dangerous-loopholes/
244 Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf
245 Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf

DIGITAL RIGHT	STRENGTH	WEAKNESS
Freedom of thought, conscience and religion	By banning AI systems that are considered to pose an unacceptable risk via manipulation, the Act protects freedom of thought.[246]	Critics highlight that the AI systems that are banned on the basis of manipulation are decided using a very narrow criteria. These systems are banned if they use 'subliminal techniques or exploit the fragility of vulnerable individuals and could potentially harm the manipulated individual or third person.'[247] The AI Act does not consider manipulation as a result of the extensive reliance on user data which can exploit people's cognitive differences.[248]
Non-discrimination	The partial ban on biometric identification takes a step towards protecting the right to non-discrimination.[249] Mandatory fundamental rights impact assessments, that must be summarised publicly, will hold deployers of AI systems accountable to the article of non-discrimination.[250] High risk AI systems must comply with accessibility requirements to support their use by people with disabilities.[251]	The ban on biometric identification is considered partial as it is still available for use by law enforcement, and the suspicion of any crime justifies its use.[252] Whilst the categorisation of biometric data based on race, political beliefs and sexual orientation are prohibited, other forms of categorisation, such as gender, are still allowed.[253] Whilst high risk systems must comply with accessibility requirements, limited and minimal risk systems do not. This limits the commitment to protecting against non-discrimination for people with disabilities.[254]

246 Vieth-Ditlmann, K. and Aszodi, N. A guide to the AI Act, the EU's new AI rulebook. Algorithm Watch, 2024. https://algorithmwatch.org/en/ai-act-explained/
247 Franklin, M., Ashton, H., Gorman, R. and Armstrong, S. The EU's AI Act needs to address critical manipulation methods. OECD.AI Policy Observatory, 2023. https://oecd.ai/en/wonk/ai-act-manipulation-methods
248 Franklin, M., Ashton, H., Gorman, R. and Armstrong, S. The EU's AI Act needs to address critical manipulation methods. OECD.AI Policy Observatory, 2023. https://oecd.ai/en/wonk/ai-act-manipulation-methods
249 Vieth-Ditlmann, K. and Aszodi, N. A guide to the AI Act, the EU's new AI rulebook. Algorithm Watch, 2024. https://algorithmwatch.org/en/ai-act-explained/
250 European Centre for Not-for-Profit Law. Big Win for Fundamental Rights, As The European Parliament Adopts The AI Act. 2023. https://ecnl.org/news/big-win-fundamental-rights-european-parliament-adopts-ai-act; Muller, A. and Spielkamp, M. AI Act deal: Key safeguards and dangerous loopholes. Algorithm Watch, 2023. https://algorithmwatch.org/en/ai-act-deal-key-safeguards-and-dangerous-loopholes/
251 Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf
252 Vieth-Ditlmann, K. and Aszodi, N. A guide to the AI Act, the EU's new AI rulebook. Algorithm Watch, 2024. https://algorithmwatch.org/en/ai-act-explained/
253 Vieth-Ditlmann, K. and Aszodi, N. A guide to the AI Act, the EU's new AI rulebook. Algorithm Watch, 2024. https://algorithmwatch.org/en/ai-act-explained/
254 Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf

DIGITAL RIGHT	STRENGTH	WEAKNESS
Non-discrimination		The Act allows for national security to be used as a justification for the use of biometric mass surveillance systems without any safeguards such as fundamental rights impact assessment, high technical standards, and assured anti-discriminatory practice.[255] Whilst there are measures in place to mitigate against AI system bias, there is no strict condition that requires AI systems to be unbiased. AI pre-selection increases the likelihood of a biassed outcome, even with risk mitigation factors such as post-hoc human verification, which can still be liable to bias.[256]

255 Joint Statement. EU's AI Act fails to set gold standard for human rights. Algorithm Watch, 2024. https://algorithmwatch.org/en/wp-content/uploads/2024/04/Cover_Joint-Statement_AI-Act_3-April-2024.pdf
256 Arnold, L. How the European Union's AI Act Provides Insufficient Protection Against Police Discrimination. PennCareyLaw, 2024. https://www.law.upenn.edu/live/news/16742-how-the-european-unions-ai-act-provides

CS 3.2 Global approaches

The Global Digital Compact and Council of Europe AI Treaty establish significant frameworks for governing AI systems and algorithmic interactions. The Global Digital Compact dedicates Objective 5 specifically to AI governance, stating that parties must "enhance international governance of artificial intelligence for the benefit of humanity."[257] Key provisions include:

- ***Article 50:*** *We recognize the need for a balanced, inclusive and risk-based approach to the governance of artificial intelligence (AI), with the full and equal representation of all countries, especially developing countries, and the meaningful participation of all stakeholders.*[258]

On oversight and transparency, the GDC mandates:

- ***Article 55d:*** *Promote transparency, accountability and robust human oversight of artificial intelligence systems in compliance with international law.*[259]

The Council of Europe AI Treaty provides more detailed obligations:

- ***Article 16:*** *adopt or maintain measures for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems by considering actual and potential impacts to human rights, democracy and the rule of law.*[260]

On risk management, such measures must:

- ***Article 16 (2ba):*** *take due account of the context and intended use of artificial intelligence systems.*[261]
- ***Article 16 (2b):*** *take due account of the severity and probability of potential impacts.*[262]
- ***Article 16 (2c):*** *consider, where appropriate, the perspectives of relevant stakeholders, in particular persons whose rights may be impacted.*[263]

257 United Nations (2024) Global Digital Compact, Objective 5.
258 United Nations (2024) Global Digital Compact, Art 50.
259 United Nations (2024) Global Digital Compact, Art 55d.
260 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 16.
261 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 16 (2a).
262 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 16 (2b).
263 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 16(2c).

APPROACHES BY THE GOVERNMENT OF THE REPUBLIC OF SOUTH KOREA

In South Korea, the Digital Bill of Rights has committed to the ethical development of new technology.[264]

- ***Article 8 Respect for Digital Diversity:*** *Every individual shall be protected from unjust discrimination and bias arising from digital technology and shall be respected for their social and cultural diversity*
- ***Article 17 Ethical Development and Use of Digital Technology:*** *The development and use of digital technology shall be conducted responsibly in an ethical manner to ensure safety and trust.*

The primary policy action pledged by South Korea is to ensure the safety, trustworthiness and ethics of AI technology is balanced with innovation.[265] It has sought to achieve this by preparing an 'Autonomous Checklist for Implementing Artificial Intelligence Ethical Standards (2022)' and the 'Reliable Artificial Intelligence Development Guide (2022)' which shares technical measures to remove bias in learning data and artificial intelligence models.

264 The Government of the Republic of Korea. (2023) South Korean Digital Bill of Rights. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=

265 The Government of the Republic of Korea. (2023) South Korean Digital Bill of Rights. https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=

CASE STUDY 4
DIGITAL SKILLS

In Chapter 3, we highlighted that digital skills has long been at the forefront of the global digital rights agenda, yet it took nearly 20 years before it began being framed as a 'right' in its own right within the EU and is yet to be positioned in such a way in the UK.

CS 4.1 European digital skills policy approaches

The European Declaration on Digital Rights and Principles stipulates that:

- *Everyone should be able to acquire the education and skills necessary to enjoy the benefits of digital technology*[266]

To achieve this, via the EU's Digital Decade programme, the EU has set itself a target of at least 80% of those aged 16-74 have at least basic digital skills by 2030.[267,268] Basic digital skills include: information and data literacy; communication and collaboration; digital content creation; safety; and problem solving.[269] By this measure, in the EU just over half (56%) of individuals have basic digital skills, although this varies significantly between member states, from 83% in the Netherlands to 28% in Romania.[270] The Commission has stated that reaching the 80% target is a major challenge, and that without further action, only 59.8% of the population would have at least basic digital skills by 2030 based on the current trajectory.[271]

At the EU level, there is also the Digital Education Action Plan.[272] It includes recommendations to member states to set overarching objectives for provision of digital skills; to promote digital skills in schools; and to support the development of digital skills of adults, including by providing "specific support for those adults most in need of developing their digital skills".[273] Examples of current initiatives include the Digital Skills and Jobs Coalition which aims to "tackle the digital skills gap by bringing together Member States, companies and organisations".[274] The Commission is also exploring the possibility of introducing a European Digital Skills Certificate.[275] The EU is also funding digital skills development through the Digital Europe

266 European Commission "European Digital Rights and Principles". Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/digital-principles.
267 European Union (2022) "Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)". EUR-lex. https://eur-lex.europa.eu/eli/dec/2022/2481/oj.
268 It at also seeks to achieve at least 20 million ICT specialists employed within the Union, while promoting the access of women to this field and increasing the number of ICT graduates which is not the focus of this section.
269 European Commission (2024) "DESI Indicators". Shaping Europe's Digital Future .https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators?period=desi_2024&indicator=desi_dsk_bab&breakdown=ind_total&unit=pc_ind&country=AT,BE,BG,HR,CY,CZ,DK,EE,EU,FI,FR,DE,EL,HU,IE,IT,LV,LT,LU,MT,NL,PL,PT,RO,SK,SI,ES,SE.
270 Ibid.
271 European Commission (2024) "2024 State of the Digital Decade Package", Annex 1, 3.1.1. . https://digital-strategy.ec.europa.eu/en/policies/2024-state-digital-decade-package.
272 European Commission. "Digital Education Action Plan - Action 1". European Education Area. https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-1.
273 European Union (2023) "Council Recommendation of 23 November 2023 on improving the provision of digital skills and competences in education and training". Eur-Lex. https://eur-lex.europa.eu/eli/C/2024/1030/oj.
274 European Commission "Digital skills and jobs coalition". https://digital-strategy.ec.europa.eu/en/policies/digital-skills-coalition.
275 European Union (2023) "Council Recommendation of 23 November 2023 on improving the provision of digital skills and competences in education and training". Eur-Lex. https://eur-lex.europa.eu/eli/C/2024/1030/oj.

Programme, Erasmus+, the European Social Fund Plus and about 18% of the Recovery and Resilience Facility digital expenditure (EUR 23 billion).[276]

Individual member states have their own national strategies, programmes and action plans which outline the overall approach to improving citizens' digital skills.[277] In aggregate, member states have committed to investing EUR 25 billion to programmes to improve basic digital skills.[278] These include "digital skills in formal education and upskilling and reskilling programmes for people currently in employment, to actions addressed at vulnerable groups".[279] However, there are concerns that these programmes are not reaching the people with the least digital skills, such as vulnerable groups, the older population, people with little or no formal education, people living in rural areas and people with disabilities.[280]

English digital skills policy[281]

Among school-age children, 'computing' is already a compulsory part of the national curriculum, and this includes some aspects of digital skills and digital literacy such as using the internet safely, online identity and privacy.[282] The number of hours dedicated to computing or digital skills has fallen significantly since 2010, and there is a significant gender gap with girls constituting one in five (21%) of entries for Computer Science GCSE.[283] There is also no requirement for students to reach a minimum qualification level in computing by age 16. Post-16, while digital skills are available as part of a variety of intermediate (Level 3) qualifications, including T Levels and apprenticeships, there is no obligation to pursue these.[284] The curriculum is currently under review by the government via a 'Curriculum and Assessment Review' and so may yet widen to improve emphasis on digital skills.

The UK Digital Strategy (2022) describes the last government's commitments to advancing digital skills, including among adults and vulnerable groups.[285] A particular focus had been on strengthening 'essential digital skills', using The Essential Digital Skills Framework (2019) to guide basic courses/qualifications (Entry Level and Level 1) provided for free to adults aged 19+ in England via Further Education colleges, local government adult education services and independent training providers.[286,287] The new government, in 2024, established Skills England, a new body designed to "bring together central and local government, businesses, training providers and unions to meet the skills needs of the next decade across all regions, providing strategic oversight of the post-16 skills system".[288] The first report published by Skills England highlights that 8% (4.4 million) people lack 'Essential Digital Skills for Life', and 18% (7.4

276 European Commission (2023) "2023 Report on the state of the Digital Decade". https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade.
277 Publications Office for the European Union (2024) "Study to support the monitoring of the Declaration on Digital Rights and Principles". European Commission. https://op.europa.eu/en/publication-detail/-/publication/19168f56-2ebd-11ef-a61b-01aa75ed71a1/language-en.
278 European Commission (2024) "2024 State of the Digital Decade Package", Annex 1. https://digital-strategy.ec.europa.eu/en/policies/2024-state-digital-decade-package.
279 Ibid.
280 Ibid.
281 Digital skills policy is different in England, Scotland, Wales and Northern Ireland so we focus on just in England here
282 Department for Education (2014) "National curriculum in England: framework for key stages 1 to 4". https://www.gov.uk/government/publications/national-curriculum-in-england-framework-for-key-stages-1-to-4/the-national-curriculum-in-england-framework-for-key-stages-1-to-4.
283 Kemp, P., Wong, B., Hamer, J. and Copsey-Blake, M. (2024) "The Future of Computing Education: Considerations for Policy, Curriculums and Practice". King's College London. https://epi.org.uk/wp-content/uploads/2022/11/Digital-Skills-Divided-Technical-Provision-for-16-to-19-Year-Olds-2022.pdf.
284 Ibid.
285 Department for Digital, Culture, Media and Sport (2022) "UK Digital Strategy". https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy#s3.
286 Department for Education (2019) "Essential digital skills framework". https://www.gov.uk/government/publications/essential-digital-skills-framework/essential-digital-skills-framework#introduction
287 Department for Education (2024) "Fully-funded qualifications for adults with low digital skills". https://www.gov.uk/guidance/free-qualifications-for-adults-with-low-digital-skills.
288 https://www.gov.uk/government/news/skills-england-to-transform-opportunities-and-drive-growth

million people) of non-retired adults lack 'Essential Digital Skills for Work'.[289,290] With a stronger single view of the skills needs and gaps across the country Skills England aims to inform and strengthen existing approaches, such as increasing uptake of publicly funded essential digital skills courses/qualifications, and for businesses to invest in training and upskilling for employees within the workplace.[291]

CS 4.2 Global approaches

Both global frameworks establish provisions for digital skills and literacy as essential components of digital rights.

The Global Digital Compact addresses digital skills comprehensively under Articles 12 and 13, recognizing that *"to fully harness the benefits of digital connectivity, we must ensure that people can meaningfully and securely use the Internet and safely navigate the digital space."*[292,293]

Specifically, it commits parties by 2030 to:

- ***Article 13a:*** *establish and support national digital skills strategies, adapt teacher training and education curricula and provide for adult training programmes for the digital age. Our aim is maximum coverage of basic digital skills for as many as possible, while also advancing intermediate or advanced digital skills.*[294]
- ***Article 13b:*** *increase the availability, accessibility and affordability of digital technology platforms, services, software and educational curricula in diverse languages and formats, as well as accessible user interfaces for persons with disabilities.*[295]
- ***Article 13c:*** *Target and tailor capacity-building for women and girls, children and youth, as well as older persons, persons with disabilities, migrants, refugees and internally displaced persons, Indigenous Peoples and those in vulnerable situations.*[296]

The Council of Europe AI Treaty addresses digital skills through:

- ***Article 20:*** *Each Party shall encourage and promote adequate digital literacy and digital skills for all segments of the population, including specific expert skills for those responsible for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems.*[297]

289 Lloyds Bank (2023) "2023 Consumer Digital Index". https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/231122-lloyds-consumer-digital-index-2023-report.pdf
290 Department for Education (2024) "Skills England: driving growth and widening opportunities". https://assets.publishing.service.gov.uk/media/66ffd4fce84ae1fd8592ee37/Skills_England_Report.pdf.
291 Lloyds Bank (2023) "2023 Consumer Digital Index". https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/231122-lloyds-consumer-digital-index-2023-report.pdf
292 United Nations (2024) Global Digital Compact, Art 12.
293 United Nations (2024) Global Digital Compact, Art 13.
294 United Nations (2024) Global Digital Compact, Art 13a.
295 United Nations (2024) Global Digital Compact, Art 13b.
296 United Nations (2024) Global Digital Compact, Art 13c.
297 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 20.

APPROACHES BY THE GOVERNMENT OF THE REPUBLIC OF SOUTH KOREA

In the South Korean Digital Bill of Rights stipulates:[298]

- ***Article 14 the 'Enhancement of Digital Literacy':*** *The digital divide shall be bridged to ensure opportunities for the development and use of digital technology, and educational opportunities shall be provided for the improvement of digital literacy.*

The South Korean government seeks to tackle the digital divide with policy approaches that focus on school-level education, including: doubling the amount of lesson time for elementary and middle school information education through revising the curriculum, providing additional teaching and learning materials, such as 'AI digital textbooks' and providing additional AI-based training for teachers in line with the introduction of the curriculum.[299] It also aims to establish 1,000 leading schools in digital education with '500 AI-centric' schools.

298 The Government of the Republic of Korea (2023) "South Korean Digital Bill of Rights". https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=
299 Ibid.

CASE STUDY 5
DIGITAL ACCESS

Like digital skills, digital access has also long been at the forefront of the global digital rights agenda.

CS 5.1 EU digital access policy approaches

The EU made a strong commitment to accessibility, as outlined in the European Declaration on Digital Rights and Principles, committing to:

- ***Article 3:*** *Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity.*

While overall connectivity has improved across the EU in recent years, with fibre networks now reaching 64% of households, there are persistent regional disparities. Currently, 5G coverage only extends to about 50% of EU territory.[300] Urban-rural divides also remain prominent, with rural areas often having limited access to high-speed broadband and 5G networks.[301] The EU has deployed significant funding through initiatives like the Connecting Europe Facility (CEF) Digital, which allocates €1.7 billion for broadband expansion and the Digital Europe Programme, providing €7.9 billion to support digital infrastructure and emerging technologies.[302] However, significant funding gaps persist with a €174 billion funding shortfall, potentially leaving around 45 million EU residents without high-speed broadband by 2030.[303]

The EU Commission has urged Member States to accelerate investments in infrastructure to bridge these digital divides, emphasising the importance of cross-border collaborations and local partnerships to improve connectivity for all regions. In this spirit, several countries have launched their own initiatives to increase digital access. In France, the *Très Haut Débit* (Very High-Speed) initiative aims to provide universal access to fibre-optic broadband by 2025, with a particular focus on rural areas - supported by the EU's Connecting Europe Facility (CEF) Digital fund.[304] Similarly supported by a combination of national and EU funding, Germany implemented the Gigabit Strategy, aiming to extend gigabit-capable networks and 5G to areas lacking reliable broadband. Together, these initiatives reflect the EU's multipronged approach: providing financial support, setting regulatory frameworks, and fostering cross-border cooperation to ensure a more digitally inclusive Europe. However, the success of these efforts will depend on addressing funding gaps, streamlining infrastructure deployment, and ensuring that digital investments reach all EU citizens, particularly those in rural and economically disadvantaged regions.

300 European Commission (2024) "Second report on the State of the Digital Decade calls for strengthened collective action to propel the EU's transformation". https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_3602/IP_24_3602_EN.pdf
301 Eurostat (2024). "Digitalisation in Europe". European Commission. https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024.
302 European Commission (2024) "Second report on the State of the Digital Decade calls for strengthened collective action to propel the EU's transformation". https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_24_3602/IP_24_3602_EN.pdf
303 Arnal, J. and Ricart, R. (2023) "A Connectivity Package for the EU: considerations on digital strategic autonomy". Real Instituto El Cano. https://www.realinstitutoelcano.org/en/policy-paper/a-connectivity-package-for-the-eu-considerations-on-digital-strategic-autonomy/.
304 Global Infrastructure Hub "ICT Case Study: France - Plan France Très Haute Débit (Rural Highspeed Broadband). https://cdn.gihub.org/umbraco/media/2752/case-study-plan-france-tres-haut-debit-rural-highspeed-broadband.pdf.

The European Commission is currently exploring proposals for major internet content providers - such as streaming platforms and social media companies - to be required to financially contribute to the infrastructure costs of expanding high-speed networks.[305]

UK digital access in the UK

In the UK, the government's digital inclusion strategy is overdue for an update with the last one published over a decade ago.[306] The new government in 2024 has appointed a Minister with specific responsibility for connectivity and digital inclusion and committed to publishing an updated strategy arguing that connectivity is "as essential as water and electricity."[307] In the meantime, while 95% of the country has access to superfast broadband, this falls to 85% among rural areas (86%) and just 39% of the country have access to gigabit broadband. To address connectivity gaps created through regions under-served via digital infrastructure, the UK government had introduced Project Gigabit, a £5 billion programme to extend gigabit-capable broadband to rural and remote areas, including phased contracts for suppliers in "not-spots" (areas without commercial investment) and a Gigabit Broadband Voucher Scheme, offering up to £4,500 per eligible premise to support broadband installation costs.[308] However, targets have been revised for Project Gigabit to a target of 85% gigabit-capable coverage by 2025, down from the original goal of universal coverage, leaving some regions more isolated.[309,310]

The Shared Rural Network (SRN) was also launched by the government with a view to increasing 4G coverage across 95% of the UK by 2025.[311] It was funded in partnership with major mobile network operators (EE, O2, Three, and Vodafone) and backed by £1 billion of investment.[312] However, such a scheme fails to tackle the more fundamental issue of a lack of connectivity in peoples houses where the internet is most regularly used.[313]

Digital affordability also remains a barrier to access. 15% of 8-25 year olds live without home broadband, with connectivity and affordability of access remaining a key barrier.[314] 1.9million households continue to struggle to afford internet broadband.[315] To support greater affordability of digital access, the UK government introduced "social tariffs" - discounted broadband plans available to low-income households, aiming to make essential broadband accessible for basic online tasks like communication and accessing services.[316] However, uptake for the scheme has been low with only about 5% of eligible households enrolled. While reasons for low uptake are multi-faceted, 53% remain unaware of their availability.[317] To address the lack of take-up

305 Gahnberg, C. (2023) "Network Usage Fees: The European Commission Plays Politics with the Global Internet". Internet Society. https://www.internetsociety.org/blog/2023/10/network-usage-fees-the-european-commission-plays-politics-with-the-global-internet/
306 Government Digital Service (2014) "Government Digital Inclusion Strategy". Cabinet Office. https://www.gov.uk/government/publications/government-digital-inclusion-strategy/government-digital-inclusion-strategy
307 Byrant, C. (2024) "Sir Chris Bryant speech at Connected Britain 2024". Department for Science, Innovation and Technology. https://www.gov.uk/government/speeches/sir-chris-bryant-speech-at-connected-britain-2024; Griffith, A (2024 "Digital Technology: Disadvantaged". Department for Science, Innovation and Technology. https://questions-statements.parliament.uk/written-questions/detail/2024-10-10/8498/
308 Building Digital UK (2024) "Project Gigabit". https://www.gov.uk/guidance/project-gigabit-uk-gigabit-programme.
309 Hutton, G. (2021) "Tackling the digital divide". House of Commons Library. https://commonslibrary.parliament.uk/research-briefings/cdp-2021-0175/
310 Hennell, D. (2023) "Project gigabit evaluated: How it fails those most in need and the alternative approach required". Open Access Government. https://www.openaccessgovernment.org/project-gigabit-evaluated-how-it-fails-those-most-in-need-and-the-alternative-approach-required/168566/.
311 Shared Rural Network (2024) "BDUK Policy Paper: SRN progress update - September 2024". https://srn.org.uk/bduk-policy-paper-srn-progress-update-september-2024/.
312 Department for Culture, Media and Sport (2020) "Shared Rural Network". https://www.gov.uk/government/news/shared-rural-network
313 UK Parliament (2021) "Digital Connectivity: Rural". Hansard. https://hansard.parliament.uk/commons/2021-07-01/debates/3E57BDE2-21B0-4DB6-B1D2-97A63B2AD782/DigitalConnectivityRuralAreas.
314 Nominet (2023) "Digital Youth Index Report 2023". https://digitalyouthindex.uk/wp-content/uploads/2023/11/Digital-Youth-Index-2023-report.pdf?utm_medium=referral&utm_source=referral&utm_campaign=DYI_Report_2023&utm_content=DYI_Report_2023
315 Ofcom (2024) Communication Affordability Tracker. https://www.ofcom.org.uk/phones-and-broadband/saving-money/affordability-tracker/
316 Ofcom (2024) 'Social tariffs: Cheaper broadband and phone packages'. https://www.ofcom.org.uk/phones-and-broadband/saving-money/social-tariffs/
317 Say, M. (2023) "Ofcom and Which? Launch broadband social tariff campaign". UK Authority. https://www.ukauthority.com/articles/ofcom-and-which-launch-broadband-social-tariff-campaign/.

of existing social tariffs, Ofcom has pressed providers to enhance website clarity and conduct proactive outreach to inform eligible households.[318]

CS 5.2 Global approaches

Both global frameworks establish digital access as a fundamental right and priority, with specific provisions for universal and meaningful connectivity.

The Global Digital Compact establishes comprehensive provisions for digital access under Articles 10 and 11, committing to "connect all persons to the Internet." On connectivity, it requires parties by 2030 to:[319,320]

- ***Article 11a:*** *Develop and strengthen targets, indicators and metrics for universal meaningful and affordable connectivity, building on existing work, and integrate these into international, regional and national development strategies.*[321]
- ***Article 11b:*** *Develop innovative and blended financing mechanisms and incentives... to connect the remaining 2.6 billion people to the Internet and to improve the quality and affordability of connectivity.*[322]
- ***Article 11c:*** *Invest in and deploy resilient digital infrastructure, including satellites and local network initiatives, that provide safe and secure network coverage to all areas, including rural, remote and 'hard-to-reach' areas.*[323]

The Compact also explicitly recognizes accessibility as a core principle:

- ***Article 8g:*** *Accessible and affordable data and digital technologies and services are essential to enable every person to participate fully in the digital world. Our cooperation will promote digital accessibility for all and support linguistic and cultural diversity in the digital space.*[324]

The Council of Europe AI Treaty, while focused primarily on AI governance, includes provisions supporting digital access through:

- ***Article 7:*** *Adopt or maintain measures to respect human dignity and individual autonomy in relation to activities within the lifecycle of artificial intelligence systems.*[325]

318 Ibid.
319 United Nations (2024) Global Digital Compact, Art 10.
320 United Nations (2024) Global Digital Compact, Art 11.
321 United Nations (2024) Global Digital Compact, Art 11a.
322 United Nations (2024) Global Digital Compact, Art 11b.
323 United Nations (2024) Global Digital Compact, Art 11c.
324 United Nations (2024) Global Digital Compact, Art 8g.
325 Council of Europe (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Art 20.

APPROACHES BY THE GOVERNMENT OF THE REPUBLIC OF SOUTH KOREA

South Korea's 'Digital Bill of Rights' also includes:[326]

- ***Article 6:*** *Guarantee of Digital Access: Every individual shall be guaranteed a stable network environment and to access and use various digital services anywhere and anytime without discrimination through the same.*

The South Korean government has sought to approach this through reducing the communication fees for vulnerable groups such as disabled persons and people on low incomes through the universal service system, and has increased the number of public Wi-Fi units.[327] It has also amended the Anti-Discrimination against Disabilities Act (2021), which stipulates the guarantee of information access via kiosks and apps for disabled persons.

Digital access has only recently emerged through language of rights norms and principles in the EU more recently and is yet to be positioned in such a way in the UK. The following two sections evaluate these policy approaches in more detail.

326 The Government of the Republic of Korea (2023) "South Korean Digital Bill of Rights."https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=19&searchOpt=ALL&searchTxt=
327 Ibid.

Licence to publish

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions

a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.

d 'Original Author' means the individual or entity who created the Work.

e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.

f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b to distribute copies or phono-records of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phono-record of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended

for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

a By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

b Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

a This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

a Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

b If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d This Licence constitutes the entire agreement between the parties with respect to the Work licenced here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.

DEMOS

Demos is a champion of people, ideas and democracy. We bring people together. We bridge divides. We listen and we understand. We are practical about the problems we face, but endlessly optimistic and ambitious about our capacity, together, to overcome them.

At a crossroads in Britain's history, we need ideas for renewal, reconnection and the restoration of hope. Challenges from populism to climate change remain unsolved, and a technological revolution dawns, but the centre of politics has been intellectually paralysed. Demos will change that. We can counter the impossible promises of the political extremes, and challenge despair – by bringing to life an aspirational narrative about the future of Britain that is rooted in the hopes and ambitions of people from across our country.

Demos is an independent, educational charity, registered in England and Wales. (Charity Registration no. 1042046)

Find out more at **www.demos.co.uk**

DEMOS

PUBLISHED BY DEMOS FEBRUARY 2025

15 WHITEHALL, LONDON, SW1A 2DD
T: 020 3878 3955
HELLO@DEMOS.CO.UK
WWW.DEMOS.CO.UK