THE UNIVERSITY of EDINBURGH

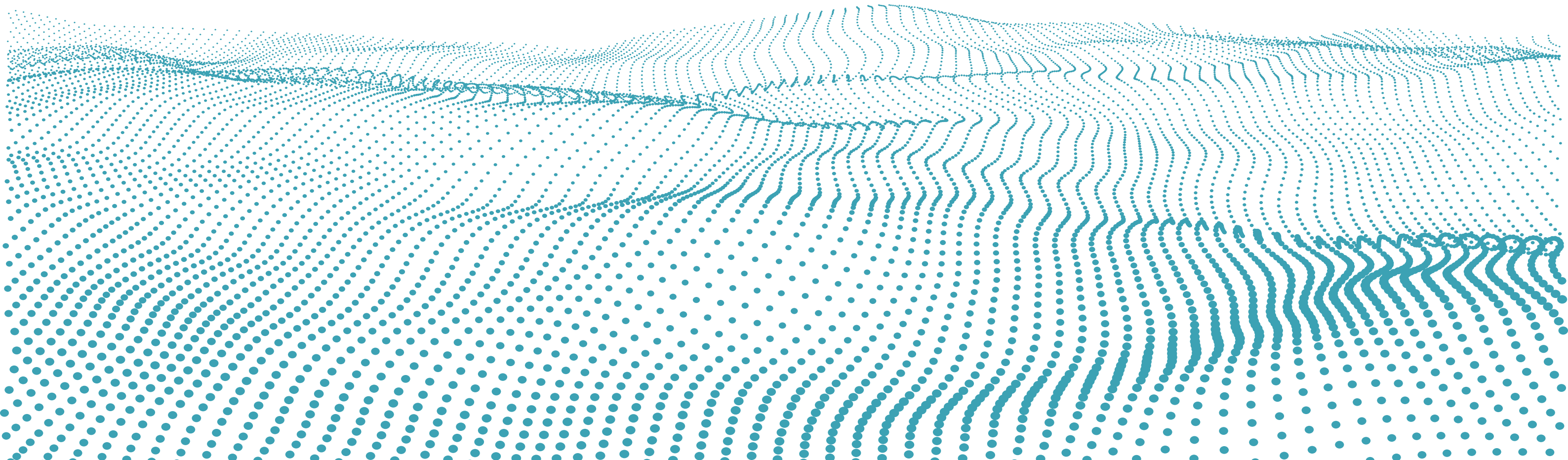
EDINBURGH INNOVATIONS

Building Trust in the Digital Era: **Achieving Scotland's Aspirations as an Ethical Digital Nation**

Digital Ethics Expert Group Report

Contents

Building Trust in the Digital Era: Achieving Scotland’s Aspirations as an Ethical Digital Nation



Acknowledgements

History of the Expert Group

The idea for a national expert group in digital ethics arose out of a set of consultation exercises by the Scottish Government's Digital Directorate in 2019 (Scottish Government, 2020) aimed at understanding the ethical challenges presented by its emerging strategy. This included a series of stakeholder consultation exercises, an informal literature search and a commissioned review of how other countries are responding to the ethical challenges presented by digital society.

Group members were selected from a wider list of experts developed by the Chair and members of the directorate. The majority of members are academics working in areas related to digital ethics, from a range of backgrounds including law, philosophy, social science, engineering and data protection. During their deliberations, the Expert Group has also reached out to national and international experts and leaders in digital technology and policy. In parallel with the expert group, the Chair and members of the Expert Group contributed to a deliberative public engagement exercise organised by Involve and Carnegie UK, including giving talks, observing the discussions and reviewing reports. This approach has helped to ensure the linkage between the local experts, a wider community of practice, and a deliberative public panel including a cross-section of people from Scotland.

The report editors owe considerable thanks to the **members of the Expert Group** and contributors who have given so freely of their time and expertise to support the building out of the broader concepts and content of the report, as well as their specific case study contributions. The Expert Group and contributors have provided a diverse range of perspectives on this foundational report, however it should be noted that the final content, conclusions and recommendations has been decided upon by the report's editors. Whilst the Expert Group and contributors are supportive of the overall aims of the report, it may not necessarily, on all details, represent the individual views of the experts or their institutions.

National Digital Ethics Public Panel (mini-public)

The National Digital Ethics Public Panel[1] brought together a broadly representative group of 30 people from across Scotland to learn, discuss and deliberate on key aspects of digital ethics. The focus was to explore how Scotland could mitigate the potential risks and harms that the growing use and reliance on digital technologies poses to individuals and to society more broadly, while maximising the benefits and opportunities. Recommendations, quotes and insights from the National Digital Ethics Public Panel have been used to inform this report and are integrated within it. The full report from the National Digital Ethics Public Panel is available to review as a separate publication, which is highly recommended to be read in conjunction with this report, for the valuable insights gained.

[1] How should Scotland best respond to the digital revolution in an ethical way? (org.uk)

Introduction

The purpose of this report is to advance the vision of an Ethical Digital Nation as set out in **Scotland's Digital Strategy** (Digital Directorate, 2021). Compiled by the National Expert Group on Digital Ethics, it aims to develop strategic and actionable **recommendations** for an Ethical Digital Scotland, informed by the best available evidence, expert knowledge and insights from multiple publics and stakeholders.

Becoming an Ethical Digital Nation is a key ambition for the Scottish Government. The Digital Strategy states that:

> **“ Our vision is for a society where people can trust public services and businesses to respect privacy and be open and honest in the way data is being used... A place where children and vulnerable people are protected from harm. Where digital technologies adopt the principles of privacy, resilience and harm reduction by design and are inclusive, fair and useful. ”**
>
> **Digital Directorate, 2021**

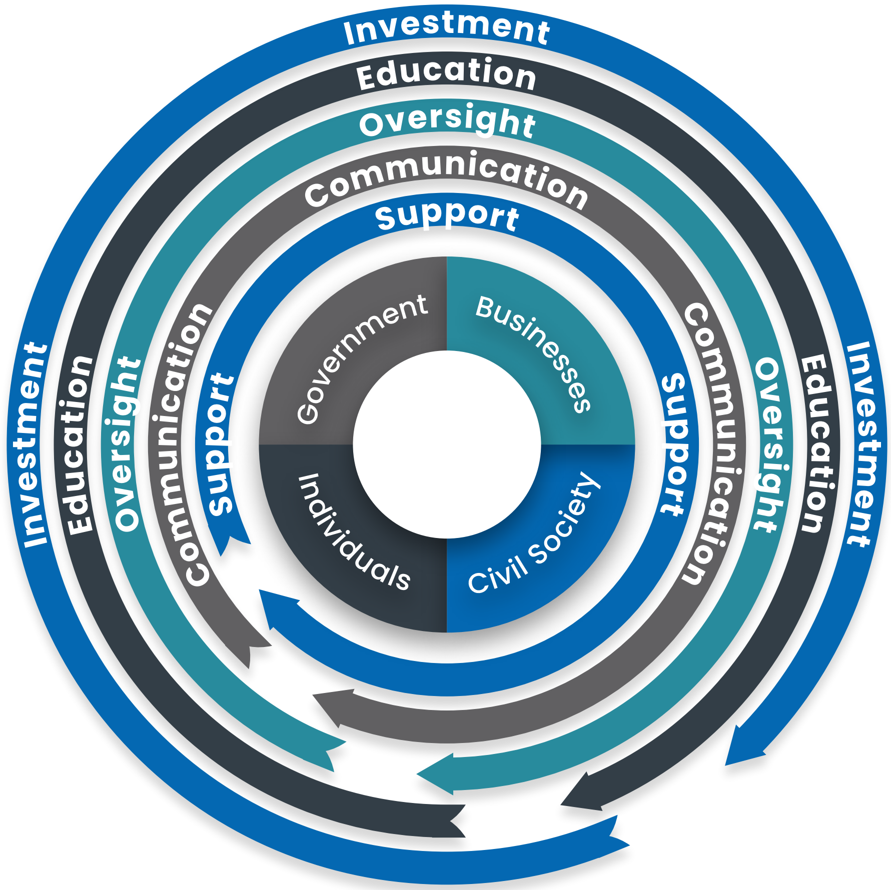
This report is the first step in setting out a vision of an **Ethical Digital Nation** as outlined in the Digital Strategy.

The outcomes of this report will help to realise the additional actions listed in the Strategy, including:

- Build public trust in the use of data
- Make more of our data available openly
- Increase community engagement and participation
- Engage with confidence on the international stage
- Realise digital rights
- Use Scotland's data capabilities to address climate change targets (Digital Directorate, 2021).

Where there is clear opportunity for citizens and society to benefit from increased use of digital in the way we live our lives, we need to be taking the necessary steps to ensure that ethics sits at the front and centre of our decision-making, across government, private sector, civil society and as citizens. Here we draw out the views expressed by the public and the expert group around some of the ethical challenges present in the digital domain.

This report makes strategic and actionable recommendations, taking into account existing activity and identifying where gaps exist or where focus should increase. These recommendations all relate to the levers available to Scotland at multiple institutional levels. The graphic below shows a summary of these levers, with the responsible owners of the recommendations noted in the middle of the diagram.



The recommendations in this report are specific to the ethical tensions explored by the expert group and the people's panel but should be considered within the context of a range of Scottish Government strategies and policies that currently support the realisation of an ethical digital nation. The most significant of these are the overarching **Digital Strategy - A Changing Nation: How Scotland Will Thrive in a Digital World**. The **AI Strategy**; which sets out a vision for AI in Scotland and the principles and actions that will underpin the development of a strong and ethical AI eco-system in addition to the **National Strategy for Economic Transformation**, the COVID Recovery Strategy and supporting policies on improving digital skills and a **Just Transition**.

A summary of the recommendations can be found at the end of this report. This summary aims to synthesise a set of recommendations based on the content of each chapter of the report and reflects the views of the Public Panel, such that each of the responsible owners can strategise on how they can set about acting on the recommendations.

This report offers a number of frameworks and concepts that can be used to help with the analysis and potential options in trying to reach an Ethical Digital Scotland. It demonstrates examples of good and bad practice throughout a number of thematic chapters.

Each section flags important elements for the individual, community, organisation and government, which focus on setting out ethical approaches to issues such as the impact of digital technologies on privacy and democracy. There will be changes and safeguards needed to maximise benefits while minimising risks and harms.

Why is this needed?

Scotland's people deserve to benefit from the opportunities the digital era can bring, such as more efficient and convenient public services, new forms of employment and opportunities to build cutting-edge businesses that grow the economy and contribute to wellbeing and environmental sustainability. The Scottish government has invested heavily developing eGovernment services as well as major digital infrastructure projects, innovation centres, and programmes aimed at encouraging start-ups and generating tax revenue. Significant successes have been seen in digital and data-driven sectors such as cybersecurity, gaming, robotics, biomedical research, and fintech, promising to create employment and support sustainability.

Despite these potential benefits, these developments also **present ethical and societal challenges and dilemmas**. For one thing, access to digital, and the skills to use it, are unevenly distributed and may potentially exacerbate inequalities, particularly as services have moved to 'digital first'. Current digital services have facilitated or been deployed in ways that has intensified or created new channels for a whole range of harms: fraud, hate crime, privacy invasion, information crimes, gambling addiction, suicide, terrorism, and structural forms of discrimination. The increasing ability to capture data from the activities of individuals and organisations, often as the basis for providing legitimate services, continues to challenge our ability to ensure fairness, privacy and rights.

The Public Panel, giving insight from Scottish citizens, reveals strong expectation for protection by government, which is also complex to deliver.

It is recognised that many of the direct legal and regulatory levers that govern digital are reserved to Westminster and managed through a range of different departments from Energy to Department of Culture Media and Sport with regulatory powers distributed between a number of bodies. Therefore engaging with appropriate UK Government Departments and ancillary bodies is key to increasing Scotland's influence and voice in delivering on the vision and ambition for an Ethical Digital Scotland.

Responsibility for Economic development and Education policy, in addition to oversight of a broad range of public bodies from academia to local government, is devolved to the Scottish Government and deliver levers to direct and influence behaviours across all sectors.

The recommendations from this report will provide a starting point for individuals, communities, organisations, and government to build an Ethical Digital Scotland.

What is Digital Ethics?

This simplified definition of digital ethics was developed specifically for the context of this report as part of the Scottish Government digital ethics discovery process.

Digital **ethics is ethics in the digital world**, where ethics is commonly defined as a system of moral principles, affecting how decisions are made that impact individuals, society and the environment. Ethics provides us with a moral map to help guide us through challenging issues. Ethics supports thinking beyond self-interest.

Digital ethics concerns behaviour, activities and decisions related to the digital world. The digital environment includes collecting, storing, publishing, communicating, using and sharing information. Digital ethics addresses morality around decision making in the digital space.

Digital ethics covers **interactions across:**

- **individuals**
- **organisations** (both public and private)
- **Communities**
- the **Environment** and
- **digital things** (such as mobile phones, the Internet, Artificial Intelligence, Internet of Things or robots).

Digital ethics may be framed as an area of study or practice in philosophy, technology design, law, social science, data protection, corporate governance, cybersecurity, democracy and social activism and more. Likewise, different sectors also have their own ways of looking at ethics, as do different governments. For example, the framework for 'responsible innovation'[2] favoured by the European Commission emphases the need for anticipatory ethics – thinking ahead to ensure that what is created today will not have unintended consequences in the future – which has been used to guide its research investments in areas like industrial automation. Similarly, 'computer ethics', 'engineering ethics' and 'robot ethics' consider issues such as ethical coding alongside broader issues such as risk and gender bias. 'Data ethics' encompasses concerns around information and its users, including privacy, control and rights.

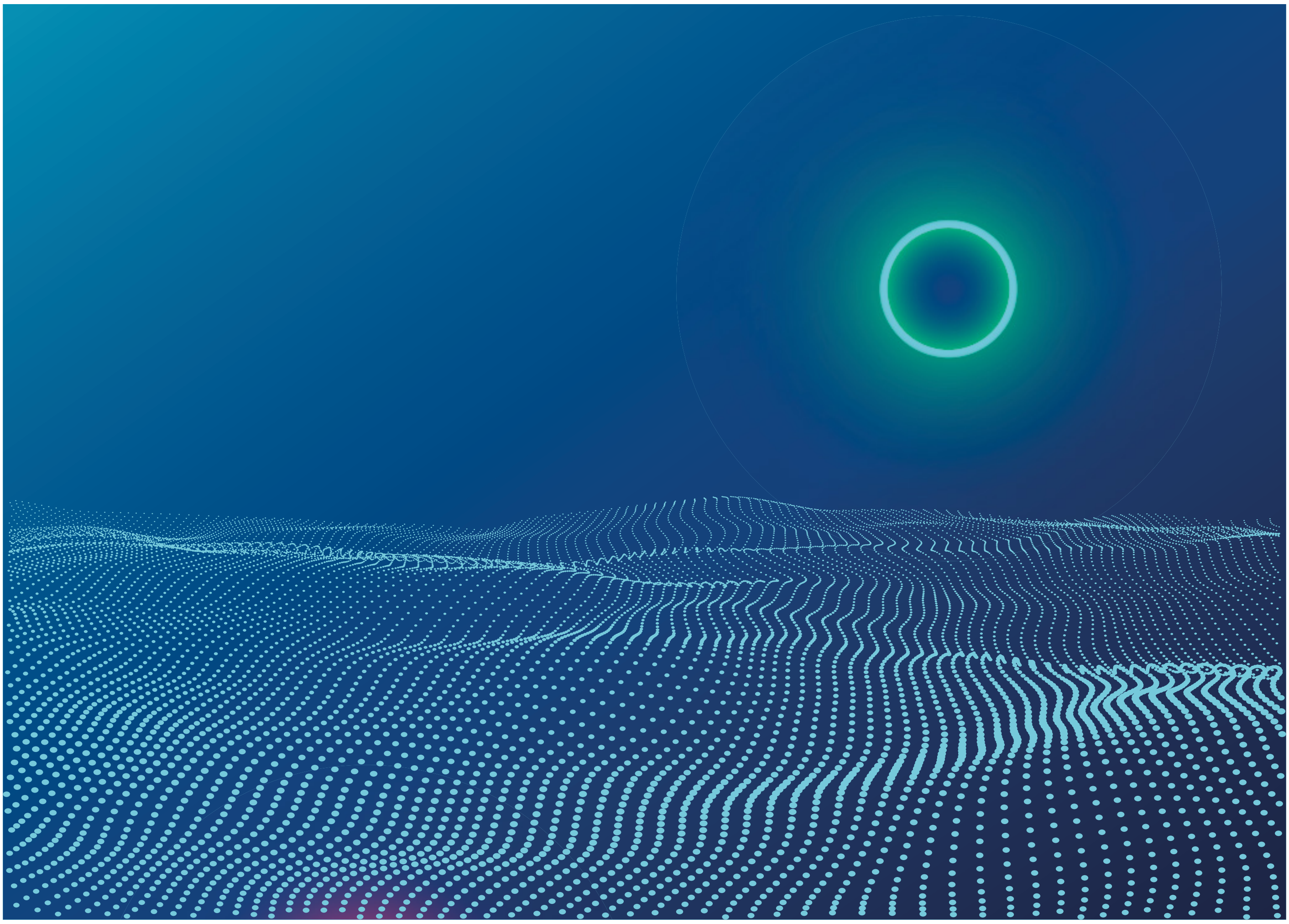
[2]. Responsible Research and Innovation in Practice (.eu)

The cluster of activity around ‘AI ethics’ includes additional considerations such as algorithmic transparency and automated injustice. Despite their nuances and priorities, recent reviews suggest that their core concepts have much in common.

Scope of Digital Ethics

The scope of Digital Ethics within this report examines issues around culture, trust and technology which:

- Covers a range of existing and emerging digital and data innovations.
- Considers how these impact people and society in different contexts e.g. health, work, education, finance, leisure, transport etc.
- Analyses risks to privacy, rights, equality, wellbeing, and the environment and how these can be overcome.
- Examines how digital may be used to support ethical and trustworthy practices through design, inclusion and accountability.
- Takes account of and seeks to inform relevant legislation, regulations and policies
- Aims to encourage a fair and responsible digital society



Frameworks and Concepts

Below are some of the key values and principles, already adopted by the Scottish Government, which ought to be considered when designing, deploying or using digital tools and services.

The National Performance Framework

Scotland's National Performance Framework is a Scottish Government tool to help Scotland create a more successful country (Scottish Government, 2018). This includes giving opportunities to all people living in Scotland, increasing their wellbeing, creating sustainable and inclusive growth and reducing inequalities.

Guiding Scotland's approach are a set of core values. These are:

- Treat all people with kindness, dignity and compassion
- Respect the rule of law
- Act in an open and transparent way

Positioning Scotland as an Ethical Digital Nation has the potential to impact across all of the National Performance Framework outcomes.

NPF Outcomes

- **Human Rights - We respect, protect and fulfil human rights and live free from discrimination.**
- **Children & Young People - We grow up loved, safe and respected so that we realise our full potential.**
- **International - We are open, connected and make a positive contribution internationally.**
- **Communities - We live in communities that are inclusive, empowered, resilient and safe.**

Objects of Trust Framework

Digital tools, products and services come in different forms and may have different functions, from the simple to the complex. They also vary in terms of who has designed or controls them, who they are targeted at, how much room for misuse there is, and what risks they present to safety, privacy, rights and freedoms. For this reason, it is not enough to ask if ‘digital’, meaning the people, the processes, the data and the technology related to digital, are trustworthy. There is a need to break the components of ‘digital’ down and consider how characteristics of trust relate to these components.

The Objects of Trust framework[3] provides one way of helping to think about the various aspects of digital innovations or services that require our trust, and the types of questions asked of different entities when trying to establish their trustworthiness. Beyond being used as a technology and software assessment tool, this framework can also be used in the context of participatory consultation processes to take account of wider ethical considerations. A fundamental requirement of an ethical approach is to consider how you will take the public view into account. The Objects of Trust framework was a key mechanism used in the consultation process with members of the Digital Ethics Public Panel as a deliberative tool.

It draws on the principles seen in other guidelines related to digital and data ethics,[4] [5] but in accessible language.

Technology Is it **reliable**? Is it **robust**? Is it **safe**?	**Usefulness** Is it **necessary**? Will it **help**? Is it **worth it**?	**Privacy** Is my information **confidential**? Are there **Laws/ Regulations** to **protect me**?	**Choice** Is it **optional**? Would **not using it prevent me** from doing **important things**?
Fairness Is it accessible to and **useable by everyone** who could benefit? Could it be used for **discrimination**? Is it **exploitative**?	**Transparency** Are the people behind it being **truthful about its purposes and beneficiaries**? Are there **other motives**?	**Institutions** Are **systems in place** to ensure effective **governance, oversight, compliance** and **accountability**?	**Users** Could it be misused to **hurt others**? Could it **harm others**? Could it **inconvenience others**?

[3] The ethics and value of contact tracing apps: International insights and implications for Scotland’s COVID-19 response

[4] EU guidelines on ethics in artificial intelligence: Context and implementation (europa.eu)

[5] Objects of Trust: The ethics and value of contact tracing apps: International insights and implications for Scotland’s COVID-19 response

The questions ask:

- Whether the **technology** itself can be trusted, in terms of reliability, robustness and safety;
- Whether it is necessary, proportionate and contributes to 'net zero', and therefore **useful**;
- Whether there are measures in place to protect **privacy**;
- Whether there is a **choice** about whether to use it;
- Whether it is **fair**, in that it's available to anyone who might benefit and doesn't lead to exploitation or discrimination;
- Whether the extent to which its true purposes are **transparent** and known;
- What **institutions** are being held to account for the design, build and operation of the technology, and finally;
- Whether there is the potential for some **users** to employ it in ways that harm or disadvantage others.

Individual objects of trust do not stand in isolation, and should be considered in relation to each other. Some of the questions will be more relevant to some digital issues than others. The questions can be adapted to a wide variety of situations. Some cases might warrant more of a deep-dive into a specific section, whereas others might benefit from a more holistic overview. The framework has been designed to support and facilitate productive discussions around the trustworthiness of various technologies.

The elements of the object of trust are linked to Scotland's approach to Fairness, and align to the values of the **National Performance Framework**.

Applying the Objects of Trust Framework as an Ethics Tool

Throughout this report, the Objects of Trust framework will be referenced at the start of each chapter. The aim is to use the framework to prompt further discussion about the issues and examples raised, and to highlight how to start thinking about the variety of components that make up a 'trustworthy' digital tool, product or service, and how we can ensure that those who are developing and deploying them can be trusted.

The framework should empower people at all levels – individual, community, organisational and governmental – to ask questions of technology and to challenge how it is designed, deployed and used.

Supplementary Information:

Data – Data is the term widely used for the information that is collected, generated, stored for reference or analysis. In the context of this report, we are talking about data held on computers and other digital machines. Data can be a value or fact associated with an individual, the environment, the economy, or data can be generated as part of the operations of computer systems that power the digital world.

Technology – There is value in separating trust in technologies themselves, from their applications, users, data or governance. People do literally trust and rely on 'things', like assistive robots or apps but this is linked to belief in the resilience, robustness, safety and validity of those 'things'. When these 'things' fail, so does trust and that break in trust goes beyond the technology itself and to the wider set of components that have contributed to that failure.

Usefulness – Sharing one's information may be necessary to obtain the full benefits of a digital product or service. To help users decide what trade-offs they are willing to make between privacy and usefulness, organisations should explicitly state how this data will be used and the limits around its usage.

Privacy – It is key that there is clarity around what information will be shared, with whom, and for what purpose. Privacy policies need to be adequately explainable and accessible to users. Only the minimum necessary data should be captured and recorded. As well as due consideration on consent and anonymization.

Freedom of choice – Are citizens free to choose whether or not to participate and to what extent? Choosing not to provide information to certain companies, or in certain circumstances, can limit your ability to access products and services. For example, during the COVID-19 pandemic, digital vaccine certificates were essential for some international travel and many people therefore used them despite concerns about surveillance. A victim of cyber-bullying may resist calls to delete their social media account if this is also a vital communication tool and digital archive for them.

Fairness – with regards to availability and accessibility to anyone who might benefit (digital inclusion) and doesn't lead to exploitation or discrimination; for example when data is used in algorithms there may be a risk that it is used in discriminatory ways, such as in automated CV screening processes, which draws scoring from previously successful applicants, thereby inheriting historical biases.

Transparency – The motives of the people and organisations driving the development of digital and data usage can influence trust in products and services. Transparency and clarity can be important to reduce perceived risks about adopting new digital services.

Institutions – This is about the authorities or agencies whose job it is to ensure the ethical oversight of digital services or projects. This may be government entities, or others (i.e. schools).

Users – This refers to other citizens who may be using the same platforms or technologies as you. In the case of digital contexts, there is concern that some people, such as anonymous trolls on Twitter, would misuse them to maliciously harm others. It is about recognising that bad actors may also be people like ourselves, and then deciding if we can still trust a digital service even when these risks are known.

Taking a Closer Look at 'Fairness': The 'Four Fairs'

There are multiple ways to define "fairness" across different sectors of digital. The 'Four Fairs' outline priorities to embrace concrete practices, safeguards and monitoring mechanisms around access, equality, diversity, inclusion, awareness/education, uptake and engagement.

Fair Society

Ensuring that the benefits of digital innovation are equitable, inclusive and accessible to all. Enabling choice and control by the citizen and putting place preventions to digitally led discrimination. Fostering responsible and environmentally sustainable innovation. Protecting human rights.

Fair Economy

Fostering a thriving digital economy in Scotland that can create jobs, grow innovation and generate tax revenues, while prioritising business sectors and models that are ethical and benefit Scotland's citizens. Ensuring transparency and accountability in digital procurement to ensure responsible guardianship of public finances and support sustainable services. Prioritising digital/data innovations that avoid environmental damage and contribute to a green future. Seeking for the benefits of digital work and business to reach all sectors of society.

Fair Technology

Avoiding digital technologies (including devices and platforms), methods and business models that are behaviourally or psychologically manipulative, unsecure, privacy invasive, financially or otherwise exploitative, or harmful or hurtful to individuals, groups or society. Being sensitive, responsible, proportionate and pro-social in the use of data. Ensuring legal and regulatory compliance, which intersects with ethics but is not the same.

Fair Government

Ensuring transparency, accountability, integrity and trustworthiness. Always prioritising the needs of the citizen and society. Making best use of public resources for public services. Promoting good-governance in the procurement of digital tools, services and research. Ensuring uses of technology and data to avoid discrimination. Promoting that digital policies, codes of practice, regulations and laws are ethically robust and actionable.

Trust as the Basis of a Thriving Digital Society

Scholars, policymakers and citizens' advocacy groups are becoming broadly aligned around the understanding that public trust is the essential ingredient for a successful digital society. Alongside the National Performance Framework, this report refers to the Objects of Trust framework – which draws on multiple concepts and principles represented in the digital ethics literature. Initially developed to understand the tensions at play around the governance of apps and data infrastructure during COVID-19[6], this recognises the different features (or objects) of a digital technology, service or programme which call for trust, each of which is linked to a set of questions that can be adapted for different problems. It considers aspects of the digital innovation, the individuals and organisations behind its development and procurement, the degree to which its purpose is sufficiently transparent, whether it is accessible and inclusive, whether it protects rights, whether it is legal, the integrity of its leaders, and the strength of the institutions responsible for its governance.

In work with the National Digital Ethics Public Panel, it was found that the Objects of Trust map well with the concerns, questions and priorities citizens spontaneously raise, and provides an accessible way of considering these issues at a general and specific level. It also maps with important UN goals for Sustainable Development, chiefly the need for strong institutions (SDG16) (United Nations Department of Economic and Social Affairs, 2022), as the bedrock of good governance, referring to the ethical exercise of power in the interests of citizens or customers, and the prioritisation of efficient, effective, equitable, legal, inclusive, and participatory innovation. These also map to standards in public life and the civil service code of conduct, as has been illustrated by recent debates over procurement of technologies and services during the COVID-19 crisis.

[6] The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response

Public Awareness of Data Use and Sharing

Objects of Trust:

Users: Could it be misused to hurt others?

Privacy: Is my information confidential?

Usefulness: Is it necessary? Will it help? Is it worth it?

What is Public Awareness of Data Use and Sharing?

Public awareness of data use and sharing is ensuring that any processes for which data about individuals is collected, used and stored are transparent and explainable to all. Rules about the preservation of individuals' privacy and about the ways in which organisations may use personal information, are laid out in UK data protection laws. However, many people tend to not understand these protections or trust them. Public trust should be one of the most important elements of an Ethical Digital Nation, and this can only be achieved if the public have a good awareness and understanding of how their personal data is used and shared, and their rights relating to data.

Personal data should be shared in a trustworthy way, aligning to broader societal values and expectations. It is not just about communicating how data is being used, but taking one step further to think about public acceptability and having the autonomy to challenge and question how their data is being used and shared. This equates to enabling a level of personal control over our personal data, which exists as a right enshrined in law already.

To promote public awareness about data use and sharing, there is a need for organisations to make sure that people understand how this data is collected and used and what steps they can take to control this and protect themselves. Better understanding and awareness will help to foster trust in businesses and governments when using personal data. Additionally, supporting the growth of trusted data intermediaries, whose roles is to manage digital data as a resource for public benefit, can facilitate trustworthy data sharing.

Why is Public Awareness of Data Use and Sharing Important?

A digital footprint is all of the information captured and collected about an individual that exists as a result of digital activity. This means that citizens are leaving behind a ‘digital trail’ of data every time they log on, use an app, swipe a card or click on a link.

There is a growing awareness of the fact that data shared online can be used to profile and target users, but a limited understanding of how this happens. Data can be shared both knowingly, for example when setting up a social media account, or unknowingly, via cookies, trackers or even store loyalty cards. It is the quantity of data points that are gathered that is increasingly becoming a concern.

Improving public awareness of data use and sharing will strengthen public trust in the institutions and services that look to use their data in an ethical way. Citizens are concerned that sharing their data could lead to it being misused. It is important that there is widespread understanding of how online platforms can be used to collect personal data, and how that can be used to deliver services. This can help empower individuals and communities to scrutinise technologies if they are being used unethically. It is not purely the responsibility of the citizen to understand more about data use and sharing, but there needs to be step change in how the organisations who are using and sharing data are more transparent and have more explainability around their processes.

Some key concerns of The Public Panel are:

- Data being sold or shared with other organisations
- Being used to target advertising
- Being used to profile individuals or groups.

(National Digital Ethics Public Panel Insight Report, 2021)

Case study >

> **“ I know that practically any website I go to will have access to things they shouldn’t, which they can then sell, or will simply be taken from them in turn. I’m resigned to my data being harvested to an extent. ”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 42**

Case Study:

Targeted advertising, advanced marketing and behaviour change

Dr. Ben Collier, Dr. James Stewart

Contemporary forms of digital marketing are the financial lifeblood of the Internet. Most of the online platforms, search engines and social media sites we use are provided free to the end user, generating revenue through the collection of intimate behavioural data, which are used to generate advertising profiles. These profiles allow adverts to be targeted and personalised not only based on demographic characteristics and traditional segmentation, but on previous and current behaviour, surfaced by the application of algorithmic technologies to extremely intimate and fine detail records of online browsing, communication, and activity. The targeted digital advertising industry has been the subject of a series of scandals and critical debates in recent years, not only due to concerns around intrusive corporate surveillance, but also in the use of this surveillance influence infrastructure for legitimate and subversive political communication. We have recently identified a new area of potential concern: the increasing use of these infrastructures by government to shape the behaviour of the public.

Government communication practices are not static, and change and adapt in line with the cutting edge of industry practice. These practices involve not only classic forms of awareness-raising – public health and safety, regulatory changes, democratic participation etc., but attempts to directly shape the behaviour of the public – often through 'nudge' and other approaches incorporating insights from behavioural science. As digital marketing tools have evolved, government departments and law enforcement are increasingly using them in behaviour change campaigns as part of a shift to prevention. This in theory allows government to shape behaviour in-the-moment in novel, intimate, and deeply targeted ways, bringing together administrative data, marketing data, and platform targeting data to target, deliver, and evaluate complex campaigns.

The use of government administrative or survey data to develop targeting profiles may be contested where those data are explicitly not to be used for marketing purposes. This blurs the line between marketing and service delivery. Secondly, the algorithmic targeting of adverts leaves open legal room to challenge if it can be proven that it has the potential to harm or disadvantage. Another concern in this domain are the unintended consequences of these campaigns, which the Scottish Government are actively tackling.

The public are largely aware of the existence of digital targeting, and as a result, may feel anxious if they receive government adverts, which they assume are as a result of their online behaviour. This presents a real capacity for unintended harm, particularly for more vulnerable groups. This is linked to the wider issue of communications 'blowback' – in which unintended consequences (such as the advert resulting in the opposite of the intended outcome for a small percentage of viewers, or accidentally spreading rather than countering false information) can result from the complex social environment in which these communications are consumed. Additionally, there are a set of issues around privacy/intrusiveness. These practices open up to government a new generation of detailed data sources that can be used to target communications by interposing a private entity (the platform). This allows for the use – at arm's length – of very intimate targeting and delivery approaches in ways not historically available to government.

Scotland and the Scottish Government are in many ways leading in developing the ethical accountable use of digital targeting approaches, with behavioural ad campaigns handled through a single centralised team and subject to ethical scrutiny and oversight. There is an opportunity to firmly develop a positive and distinctly Scottish approach to strategic communications – particularly foregrounding the values of co-production and 'bottom-up' policymaking, rather than the 'top- down' campaigns run with little public consultation, oversight, or transparency which characterise practices in many other jurisdictions (particularly in national security contexts). There remains a big challenge in terms of systemic change. Currently structures and practices are still fairly informal and there is a need for more concrete structures for accountability and governance over institutional practices.

Potential policy proposals here could include a public register of current and previous 'behaviour change' campaigns conducted by the public sector, with details of targeting and procurement, and the further formalisation of expert review (possibly in the style of the data sharing scrutiny boards used by the statistical profession within Scottish Government). As these practices become more widely spread there are also political and democratic questions to answer – such as whether micro-targeting is appropriate for use at all by the public sector – which require further scrutiny by politicians, civil society, and the public.

How can we strengthen and assure public trust in the use of data by public and private organisations?

Data can be an extremely useful tool for decision-making and service optimisation. It can help to personalise online services and advertising in line with past behaviours or predict demand for services in the future. Data is critically useful as we look to develop the quality of public services through sharing information for initiatives such as 'Smart Cities.'

Data sharing – the ability to distribute sets of public or private sector data with multiple users or applications to benefit citizens, whilst maintaining data privacy and security. However, in order to do this sustainably, there is a need to develop stronger safeguards around data collection and use. Innovative ways to use computers and data will often challenge the existing balance of interests and rights in society, politics and the economy, such that we require mechanisms of debate and governance that enable these to be decided on democratically.

There is a need for the public to be able to hold organisations and institutions, such as the NHS, to account over how their data is used, as well as having more insight and control over their data. By promoting more transparent operational mechanisms, the public may feel more confident in challenging and questioning:

- Who can be trusted with their data
- Whether individuals are aware or have given consent for their data to be used
- Whether groups could be unfairly profiled
- Whether individuals could be re- identified
- The reliability of the data collected
- The comprehensiveness of the data.

(Extracted from National Digital Ethics Public Panel Insight Report, 2021)

In order to help raise public awareness of data use and sharing, there is a need to provide all citizens with the knowledge, skills and tools to safely navigate the online space and use digital technologies. This will allow them to make more informed decisions about sharing their data. In addition, citizens should be able to easily identify the ownership, and any links between, social media and other web-based platforms to allow them to have a better understanding of how their digital footprint is being used and shared.

> **“ Acceptability depends on 3 factors:**
>
> **1. Anonymous is OK if use for social benefit & agreement sought**
>
> **2. Not to benefit corporations for additional profit**
>
> **3. Trust of companies holding data can be enforced if trust to hold safe is breached ”**

National Digital Ethics Public Panel Insight Report, 2021, P. 44

Harm Protection when Online

Objects of Trust:

Privacy: is my information confidential? Are there laws/ regulations to protect me?

Fairness: could it be used for discrimination? Is it exploitative?

Transparency: are the people behind it being truthful? Are there other motives?

What Is Harm Protection Online?

Engaging online opens up a world of opportunity, but this does not come without risks and challenges. The term Online Harms refers to psychological, financial, physical and societal damage arising from our engagement with internet platforms and social media. Examples include accidental poisoning from fake medicines sold online, self-harm encouraged by toxic forums, bullying and sexual exploitation; romance scams and identity theft for financial gain, and propaganda aimed at undermining social cohesion, trust in institutions or democratic processes. This may be via direct or indirect methods, for example, consuming harmful information posted online or directly being targeted by bad actors.

There can be lots of illegal and hurtful information posted online, and this can make it difficult to feel safe when using digital services. These harms can stem from the behaviours of people towards each other online, purposeful mal-intention or through inadvertent carelessness. Personal information warrants protection in the same way online as it would offline. For example, an individual should feel just as safe logging into their online banking app to manage their finances as they would if they walked into a brick and mortar bank on the high street.

In order to be protected from online harms, there is a need to develop a culture of transparency, trust and accountability that is supported by strong regulatory practices. It is important that harmful content and behaviours do not undermine the benefits that data and digital can offer to society. This is why protection against online harms, such as child abuse and cybercrime, should be a priority for citizens, organisations and governments.

Why is Harm Protection Online Important?

Online harms can surface in many ways, and can put people at risk from serious emotional or physical damage. These harms are very real, and cannot be ignored. What users see and experience online can cause immediate and lasting impact, particularly on vulnerable groups such as children and young people, or on businesses and organisations.

Some of the ways that online harms can present are:

- Mis/disinformation
- Financial harms (e.g. scams)
- Cybercrime
- Bullying and harassment
- Data or identity theft
- Digital gambling.

Case Study:

Elections and Social Media

Prof. Shannon Vallor

As we are able to access more information, we are more at risk of harm from false and misleading information that can have devastating impacts on wider society.

One example of this is the potential impacts mis/disinformation can have on the political landscape. Online behaviours aimed at influencing political opinions and voter choices represent a substantial portion of social media activity globally and in Scotland. Social media lower many traditional barriers to political engagement. For those with a smartphone, tablet or computer, the services are free and easy to use. They do not require travel outside the home, or formal affiliation with a party or other political organisation.

However, online social media are widely recognised as contributing to a number of democratic ills: most notably, misinformation (false or misleading information shared unwittingly); disinformation (false or misleading information shared with the intent to deceive); manipulation (targeting emotional or psychological vulnerabilities of others in order to undermine their capacity for reasoned political choice) and inauthentic political behaviour (political activity that misrepresents the intentions, identity or nature of the author or authors). Of course, misinformation, disinformation, manipulation and inauthentic political behaviour are nothing new; each has been a part of political life since politics began.

However, their online manifestations on social media pose unique risks to the health of Scotland's political community, not only due to the unprecedented speed and scale of their influence, but also the potential to leverage new forms of data and increasingly sophisticated algorithmic techniques to coordinate their impact, disguise their origin, amplify their negative effects, and make them harder for authentic political actors to mitigate or resist.

Between 2018 and 2020, Facebook removed hundreds of accounts linked to the Islamic Republic of Iran Broadcasting Corporation, which were associated with suspicious online activity in numerous countries including the United Kingdom. Pages removed included Free Scotland 2014 and The British Left (Scotsman, 2018); both posted about the 2014 Scottish independence referendum. These efforts preceded the Russian foreign interference campaign associated with the Brexit referendum in 2016. In August 2018, unverified reports and opinion pieces in The Herald (Leask, 2018 & Jones, 2018) alleged that local Scottish activists may have used 'retweet bots' – spambots that use automated scripts to seek out posts to retweet – to boost the hashtag #dissolvetheunion, and to attack pro-independence Scottish women. Later that year, a report[7] commissioned by MEP Alyn Smith confirmed that Scots were a target for malign bots controlled by state and non-state actors, with between 4% and 12% of Scottish Twitter activity determined to be "potentially malign." Along with the report, a website (scotorbot.scot, currently inactive) was launched to connect people with free 'bot detection' tools. In 2020, The Times reported, "SNP cybersecurity experts have detected a rise in divisive social media posts" linked to accounts in the United States, "particularly in relation to transgender rights." (McLaughlin & Andrews, 2020)

[7] Scottish Twitter 'has a problem with bots' (Extracted from National bbc.co.uk)

So why is inauthentic online activity a serious problem for democratic health at all, given that deception and obfuscation have always been part of the political landscape? One reason is that inauthentic activity seeks to exploit cognitive biases that are antithetical to effective reasoning and deliberation – such as our tendency to be irrationally influenced by how many times we have heard an idea, or how recently we have heard it, or how closely in our social circle. When we cannot reason effectively, we cannot self-govern effectively. Nor can we effectively deliberate together with our civic fellows. Thus exploitation of these biases at online scales and speeds not previously accessible to political manipulators not only strikes at the weakest point of any democracy, it does so with far greater force than we are used to.

How to be safe online

There are so many benefits to online activity, and with 'digital by default' quickly becoming the norm it is important that all members of society have the skills and confidence to take small steps to protect themselves online, whilst balancing this with a need to ensure that businesses, technology organisations and governments are well equipped to enforce stronger regulatory processes that promote safe online practices.

Education and awareness of the types of online harm that can surface, and the steps that can be taken on the individual level to protect against these, is particularly important. Having the confidence and ability to be able to fact-check information, identify a trusted app or site or understanding what information is being shared online will help citizens to be more confident about their online activity.

Platforms, in terms of hardware and software used to host an application or service, do have a responsibility to make sure that, as far as possible, their sites and content are not promoting online harms to their users. This could be achieved in a number of ways, such as:

- Controlling advertising algorithms
- Removing harmful content automatically
- Flagging fake news, mis/ disinformation
- Having clear and user-friendly routes for reporting online abuse or harassment
- Stronger age verification for child safety.

(National Digital Ethics Public Panel Insight Report, 2021)

> **“ As users if we want to be online, we have to take responsibility for looking out for ourselves and not assuming everything is benign. ”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 33**

A ‘Green’ Digital Scotland

Objects of Trust:

Fairness: Is it accessible to and usable by everyone who could benefit?

Transparency: Are the people behind it being truthful?

What is a ‘Green’ Digital Scotland?

An Ethical Digital Nation is one that addresses the environmental impacts of its digital usage. A ‘green’ digital Scotland is a nation that is actively seeking to reduce the carbon footprint and environmental damage of its digital use and industries (National Digital Ethics Public Panel Insight Report, 2021).

Scotland’s world-leading climate change legislation sets a target date for net zero emissions of all greenhouse gases by 2045[8]. Thinking about how to embed environmentally conscious digital products and services will be critical in helping Scotland to achieve this goal. An example of Scotland’s commitment to this subject has been the convening of Scotland’s Climate Assembly, which was one of the first fully digital climate assemblies in the world.

Digital economies can have surprisingly devastating impacts on our climate and environment. Digital waste, or e-waste, and unsustainable products and practices all contribute to worsening environmental standards, whether this is through the pollution created in the manufacturing of devices, the electrical energy consumed via online gaming and streaming sites or the physical e-waste created through the improper discarding of electronic devices. In order to achieve a ‘green’ digital Scotland, we should be considering how to better raise awareness of the environmental impacts of digital devices and technologies, as well as committing to stricter rules and standards that regulate the production of digital products in an efficient and environmentally friendly way. Education, awareness and regulation will be the key tools to help foster a sustainable digital society.

Some of the factors that pose a particular challenge to a ‘green’ digital Scotland include:

- Emissions from energy intensive servers and streaming sites
- Lack of public awareness
- The need for circular business models that support recycling and reuse
- Lack of a common framework for measuring impacts (particularly embedded carbon)
- Business cultures motivated by profit
- Lack of public motivation.

[8] Climate Change Policy (gov.scot)

Why is a ‘Green’ Digital Scotland Important?

There seems to be limited public awareness of how the digital world plays a part in contributing to issues that affect the climate, such as pollution and waste. Digital technologies can provide wide-ranging benefits and opportunities to society. Some digital innovations even allow us to better understand and control our emissions. If digital technologies are here to stay, it is important that the models set up to create, produce and utilise digital tools and technologies are designed with sustainable and ethical practices at their core.

The National Digital Ethics Public Panel Insight Report highlights that being confronted with the environmental impacts caused by the use of digital technologies was a disturbing shock to many of the Members.

> **“I think most people probably want to do the right thing and are genuinely concerned about the environment and I think that building recycling into chains of production and consumption can be rectified… but when it comes to things that people do every day like binging Netflix shows or watching videos on the bus, how are we going to explain to people the damage this is leading to?”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 26**

> **“We need to be carbon costing every aspect of our economy.”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 31**

Case Study:

Digital Waste

Gerry McGovern & Dr. Laura Fogg-Rogers

The UK was the first industrial society. Which also means it was the first to emit significant quantities of CO_2. In 1751, the UK was estimated to have emitted 10 million tons of CO_2.

Digital is physical, yet it is treated like some invisible, benevolent force. Most of the waste and pollution that digital causes occurs during the manufacture of the device.

- A smartphone can be made up of hundreds of materials and many of these materials are mined in the Global South. Child and slave labour is not uncommon in this mining process.
- Many digital devices are manufactured and assembled in the Global South in working conditions not much better than sweatshops.
- After very short lives, these “old” electronics are often packed into containers and then shipped back to the Global South where they pollute the environment and sicken the people.

Less than 20% of e-waste gets recycled and much of the recycling is done “informally”. According to a 2021 study by the WHO, over 18 million children and 13 million women are involved in the ‘informal’ e-waste sector. Teenagers inhale toxic fumes as they burn cables in order to expose the precious wires, pregnant women sort through digital trash, and children as young as five are used (because of their small, dexterous fingers) to pick apart digital products that were deliberately designed so that they could not be easily disassembled.

The UK is the second worst in the world at creating e-waste, producing an average of 23.9 kg per person in 2019 , according to the UK Green Alliance. “The UK is the worst offender in Europe for illegally exporting toxic electronic waste to developing countries,” according to a report in The Guardian in 2019 (Laville, 2019).

The global average for annual e-waste production is 7.3 kg per person . What this means is that the majority of the world’s population is creating a couple of kg of e-waste a year at maximum, while the North is producing waste at a rapid rate.

With proper commitment to rules and standards, e-waste can be recycled in a way that it delivers a significant source of essential materials. It must be treated as a resource, not as waste. There are significant concentrations of copper, gold and lithium in e-waste and if digital products are correctly designed, the extraction of these materials can be highly efficient.

Can the Positive Impacts of Digital Technologies Balance out their Environmental Threats?

There is a need to balance the demand for digital technologies with environmentally responsible practices. Where possible, governments, organisations and citizens should be trying to limit the negative environmental impacts of their digital usage. However, there may be instances where digital technologies can actually help us to be more sustainable.

Advancements in digital capabilities may be able to have a positive environmental impact, and to help both individuals and organisations manage their own digital impacts. Some examples discussed in the National Digital Ethics Public Panel.

Insight Report (2021) include:

- Improvements in online conferencing tools has made working from home manageable for many, meaning there are opportunities to reduce carbon emissions that would have been caused by travelling to work, although noting that online conferencing carries its own carbon footprint
- Smart home technologies, such as smart meters, can help individuals manage and reduce their energy usage
- Smart city technologies can help with traffic management avoiding congestion and reducing emissions from vehicles, whilst being mindful of wider ethical issues of both surveillance (mentioned above) and targeting emission-reduction
- Online digital communities allow for items to be ‘shared’ rather than repeatedly recreated.

Key to reconciling the negative impacts of digital devices and e-waste on the climate is to put in place policy interventions and commit investment to all aspects of the ‘circular economy’. This entails investment in appropriate facilities as well as ensuring the right legal environment that both permits and incentivises recycling, reuse and repair. An example of this might be in design choices that facilitate reuse, such as developing products in such a way that all personal identifiable data can be easily and securely removed before the device enters the second hand market. Developing policies around the right to repair as well as mitigation of planned obsolescence would ensure that businesses were committed to minimising e-waste.

Another area of focus should be to raise awareness among citizens and businesses about the negative climate impacts of digital activity and devices. As public reliance and demand for digital technology is growing, and the climate impacts of digital often being ‘invisible’, education and awareness building are a pivotal first step in helping individuals, communities and businesses to make well-informed, climate conscious choices.

[9] Children and digital dumpsites: e-waste exposure and child health (who.int)
[10] Design for a circular economy: reducing the impacts of the products we use (org.uk)
[11] Global E-waste monitor 2020 (itu.int)

Algorithmic Decision Making

Objects of Trust

Technology: Is it reliable? Is it robust? Is it safe?

Fairness: Could it reinforce discriminatory or unfair practices?

Transparency: Are the people behind it being truthful?

What is Algorithmic Decision Making?

To achieve Scotland's vision of becoming an Ethical Digital Nation, it is important that any algorithmic decision-making be supported by reliable, fair and representative data and technologies. This means that an appropriate level of transparency and scrutiny is available for any technology-supported processes or practices used to make decisions about citizens' lives. Algorithms that impact individuals should, to a certain extent, be made transparent and accessible to help build trust in how they come to their conclusions.

Algorithmic decision-making is often reliant on large amounts of data. It uses this data, through standardised rules, to derive useful information, and infer correlations, based on historic patterns and behaviours, to support decision-making. This can result in issues in explicability, due to the complex nature of the computational techniques. This type of decision-making can happen across a wide variety of activities – from credit card approvals, to targeted advertising, to automated interviewing in recruitment processes.

These decisions can have real consequences on how people live their lives. To make sure that the decision algorithms make are trustworthy and fair, there is a need for oversight and transparency in order for the public to feel confident in the legitimacy of these decisions.

Why are Reliable, Representative Data and Technologies Underpinning Algorithmic Decision Making Important?

Algorithms can be beneficial in making processes more streamlined, efficient and fairer, both from the view of the business and the user. However, as long as algorithms are used to determine outcomes for citizens, there will be a need to ensure that accountability for the design and use of the algorithm is clearly established, particularly in the event that they are suspected to be inaccurate or unfair.

Modern algorithmic systems are never neutral: they capture goals, preferences and biases of the data input and through the design of the model itself. Unless care is taken, the algorithmic systems created using data on past behaviour reflects both the wanted and unwanted biases present in society, and can perpetuate existing societal biases. For example along the lines of gender, ethnicity, age or even the area where someone lives. Reinforcing existing societal biases can mean that already marginalised groups are further discriminated and continue to miss out on support and opportunities.

Ensuring that algorithmic decision-making is underpinned by reliable, representative data and technologies is a fundamental component of being an Ethical Digital Nation. For this type of decision making to be fair and inclusive, there is a need to reduce the risk of discrimination against individuals and groups based on unreliable or inaccurate data and technology, and to ensure greater transparency about where data being used to determine outcomes is being drawn from. Scotland's AI Strategy[12] is developing a Scottish AI Playbook that will serve as an open and practical guide to how Scotland can be trustworthy, ethical and inclusive in its use of algorithms across various scenarios.

> **“ They don’t seem to be sophisticated enough, humans are much more complex and nuanced than data and machines can ever be. ”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 47**

[12] Scotland’s AI Strategy

Case Study:

Gambling

Dr. Raffaello Rossi & Prof. Agnes Nairn

Social media advertising spent is **increasing rapidly** and the basis for many modern advertising campaigns. **Already in 2018**, the gambling industry invested a massive £149m into social media marketing – which has likely increased substantially in the past three years.

The increasing use of social media (gambling) advertising, however, raises three general concerns: **First and foremost**, most social media platforms tend to be composed of relatively young demographics. On Twitter, for example, the largest demographic group are users from **18-34 years old** (51.8% of all users). On Snapchat **82% are aged 34 or younger**. In addition, on TikTok even **60% are aged 9-24**. Any advertising posted on these platforms is therefore likely to **disproportionally affect children and young people**.

Second, the cascade of social media advertising – which is considerably cheaper to launch and thus, resulting in more adverts per pound – raises substantial challenges for regulators due to its volume. Even the CEO of the UK Advertising Standards Authority publicly admitted during a **House of Lords Committee Inquiry** that methodological challenges render it highly complex for his organisation to identify whether advertisers are targeting specific (vulnerable) groups or, indeed, even know the volume of advertising to which these groups are exposed online. The combination of regulators not being able to uncover irresponsible social media advertising activity, together with the methodological challenges of analysing this massive amount of data, could potentially create a “dark space” with no one obeying the advertising rules, no one able to monitor this, and therefore no one able to regulate or inform policy thinking **(Rossi et al., 2021)**.

Finally, and related to the previous point, current UK advertising regulations are outdated. The Advertising Standards Authority (ASA) argues that UK advertising is well regulated and under control, but the stipulation that rules “**apply equally to online as to offline advertising**” makes little sense given the 'social' characteristics and possibilities of social media that simply don’t apply to traditional media. For example, the 'snowballing' effect created when users follow and engage with social media posts from companies’ accounts only applies to social media. Through snowballing, the sender of the post (e.g. the company account) has no control who will end up seeing their post – which means it might inadvertently expose children to harmful adverts. This powerful mechanism is currently completely unregulated.

A new but highly trending social media advertising technique called **content marketing** (sometimes also 'native advertising') **raises severe issues in relation to children**. Such efforts try to bypass protective heuristics that warn users internally: Be careful, this is an advert. Instead, they are designed to create a warm fuzzy feeling or to make their audience giggle. As social media users who see such a funny post like, comment on and share it, it gains momentum – might go viral. We know from previous research that children are more affective **(Pechmann et al., 2005)** and do not have the same advertising recognition skills as adults **(Wilcox et al., 2005)**. With this new form of advertising, however, it is nearly impossible for children to immediately recognise the posts' persuasive intent – breaching a fundamental marketing pillar:

"Marketing communications should be clearly distinguishable as such, whatever their form and whatever the medium used." **(International Chamber of Commerce (ICC))**. Although content marketing poses a real danger of luring children into addictive behaviour, it is nearly completely unregulated. Currently, there are regulations set by the Committee of Advertising Practise **(CAP)** that prohibit, for example, that adverts for gambling or HFSS targets or appeals to children. However, such codes do not apply to content marketing as they are not considered as advertising by the regulator (see **CAP, 2020**). Indeed, currently advertisers in the UK can do anything they like within content marketing posts. An alcohol brand account could post content marketing ads, which include children, and a gambling brand could post content marketing ads that are obviously targeted at children. Both cases, of course, would be strictly prohibited for 'normal' (i.e. non-content marketing) advertising.

In our research we found that out of 888,745 UK gambling adverts onTwitter, around 40% were classified as content marketing **(Rossi et al., 2021)**. In a subsequent study, we found that these content marketing adverts were almost 4x more appealing to children and young persons (11-24) compared to adults: 11 out of 12 gambling content marketing ads triggered positive emotions in children and young persons – only 7 did for adults **(Rossi & Nairn, 2021)**.

Introduction to a Case Study: Video Games in Scotland: Risks, Opportunities and Myths – Dr. Matthew Barr

Video games play a role in a significant number of peoples' lives across Scotland, with UK-wide data suggesting that 86% of people aged 16-69 have played computer or mobile games in the last year (UKIE, 2020). Scotland is also a significant producer of video games, with games companies including Rockstar, Outplay, Blazing Griffin, Ninja Kiwi, No Code, Stormcloud, and many more developing games here. As both producers and consumers of video games, it is imperative that we understand the ethical and social implications associated with playing them. However, our understanding of the issues is muddied by a mixture of bad science, anecdotal reports, and ill-informed media coverage. This case example provides a balanced, evidence-based overview of the science behind games' potential impact on player well-being. As such, it looks at the relationships between video games and mental health, video games and violence, and online games and gambling. In particular, the largely positive impact of video games on players' well-being during the COVID-19 pandemic is examined, with reference to peer- reviewed research carried out by the University of Glasgow. Meanwhile, the presence of gambling in online video games – in the form of so-called 'loot boxes' – is explored, with expert legal commentary from a Scottish solicitor. **Click HERE** to read the full case study.

How Can We Hold Algorithms Accountable?

As long as algorithms are being used to determine outcomes for citizens, there will be a need to ensure that accountability for the algorithm is clearly stated, for the purposes of an event where they are inaccurate or unfair. If the algorithm is determining whether someone can access education, buy a house or get a job, they need to feel confident that the outcome is justified. It is not just the outputs that need to be considered, but also how the algorithms are deployed. They should always be applied fairly and equitably, which is best done through human oversight and appropriate, potentially participatory, governance.

There should always be a way to determine how a decision was made. However, total transparency may not always be appropriate or sufficient. Some companies may want to keep their algorithms secret to avoid competition, or sometimes the data used could be sensitive and personal, and information that warrants high levels of protection.

Promoting better regulatory practices around transparency will push companies to provide more accessible explanations of how their algorithms work. Similarly, external audits could provide an extra layer of scrutiny around algorithmic decision making that can reassure the public certain standards are being met. One of the most important considerations is to think about including a 'human-in-the-loop.' This is a human 'sense check' that helps to validate the decisions that the algorithm is making. When implemented with appropriately informed, skilled and empowered human oversight, 'human-in-the-loop' protocols can help in ensuring better situational judgement and nuance can be included in the final decision.

Digital Inclusion

Objects of Trust:

Fairness: Is it accessible to, and usable by, everyone who could benefit?

Freedom of Choice: Would not using it prevent me from doing important things?

What is Digital Inclusion?

A core requirement for Scotland to become an Ethical Digital Nation is to address digital inclusion.

Digital inclusion means that people have the capability to use digital tools for things that will benefit them day to day and in the long term. This includes making sure that people have access to the right tools and technology, as well as the ability, confidence and training to use these tools successfully. A digitally inclusive society is one where the benefits of technology are available to everyone. It also means that digital tools must not exclude people from social opportunities to flourish.

Digital inclusion is an important requirement to be able to participate in society. More and more private and public services are now turning to self-service digital first, meaning that alternative options, such as paper based or in person, are rapidly becoming unavailable. Organisations are assuming that users are able to conduct everyday activities online, ranging across all types of activity, from accessing public services and education, conducting business, banking, shopping and socialising. This can be beneficial as it means many people are now able to access and interact with digital services more quickly and efficiently than they were before, saving both time and effort. However, the move to digital first could also have quite serious consequences for those that cannot, or do not want to, connect digitally.

It should be noted that there are platforms that can be enabling for people on low incomes, such as freelance cleaners using booking platforms to manage their schedules and maximise their income, demonstrating a positive use of digital technologies by users.

Digital inclusion, as highlighted as a priority by the Public Panel

The move to digital has been largely positive for lots of members of society. It is easier and more convenient to access the services we need at the touch of a button. Digital technologies have been an exciting and inspiring source of opportunity, and a positive impact on how we live our lives.

Having reliable Internet access opens doors to social and economic inclusion. For many of us work, family, play and learning occur in hybrid forms both online and in person. As technology continues to move at a rapid pace organisations are working hard to ensure that their digital strategies and services offerings are effective, user friendly and encourage productive online engagement.

Being digitally inclusive is an important factor in achieving full societal inclusion. As such, reliable and safe digital access is deemed a necessity in everyday life. Strengthening digital inclusion strategies can help us to reduce existing inequalities in our society.

Some factors that will help Scotland to foster a digitally inclusive society are:

- Helping people to acquire the skills, knowledge and confidence to navigate the digital and hybrid spaces and processes, including in the workplace
- Ensuring that secure and trustworthy digital identity and security frameworks are adopted by all public-facing commercial and government services
- Securing access to tools and infrastructure, including broadband and mobile coverage and digital devices such as phones, laptops and PCs
- Ensuring that alternative options are available for essential services and that real personal support is available to help those who struggle with self-service online services, or who are disadvantaged by not having access to the digital tools that most of us use.

Case study >

> **“ If Scotland wishes to become a Digital First nation, then including everyone (or offering the opportunity to everyone) is vital. ”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 21**

Case Study:

Online courts

Prof. Burkhard Schafer

COVID-19 forced legal systems around the globe to move at least parts of their court procedures to an online environment. The use of online courts had found vocal advocates since the turn of the century, not just, or even mainly driven, by the need to reduce the costs of the administration of justice, but as an ethical demand to achieve several aims of the justice systems in a better way than physical courts are able to. However, there had also been significant concerns, from very specific fears of negative implications for procedural fairness to more abstract concerns, such as the importance of solemn and dignified procedures to ensure public respect and acceptance of the justice system. These hypothesised concerns, together with the natural inertia of the justice system, prevented online proceedings going ahead for a long time. The pandemic succeeded where previously, academics, NGOS and law reformers had failed.

The focus of this section are online courts and online proceedings, that is legal proceedings where the parties participate remotely and mediated by technology such as Zoom, Skype, Teams, and via mobile phones, laptops or other hardware. The discussion of online courts in this sense is often combined with a demand for better use of intelligent technologies, 'legal AI', sometimes with a view of automating parts of the litigation process. These ideas for 'enhanced' online courts will only be touched upon, though in the recommendations, it can be argued that some of the new problems that online courts can bring can in turn be mitigated by better use also of 'smart' technologies.

In particular, there has been hope expressed in the literature that online courts can increase access to justice.

This can happen by reducing barriers to access:

- A reduction in direct and indirect costs on the parties (including time and opportunity costs, such as the need by parties and witnesses to travel, arrange work or care commitments around the trial schedule etc.).
- Reduction of physical barriers that affect citizens with a range of disabilities.
- Creation of curated and sharable accounts of judicial decision making for the wider public, for instance a video recording of the decision with auto-generated subtitles. In this case, access to justice and the principle of open justice are both served.

'Enhanced' online courts in addition might provide new forms of legal support for laypeople who can't afford or are otherwise prevented from using, professional legal advice, for instance by having documents automatically checked for completeness before the trial commences, or submissions auto generated based on their input of facts. This can support the principle of equality before the law.

Other possible benefits with ethical salience include:

- More efficient and as a result faster decisions, speaking to the principle that justice delayed can be justice denied.
- A more diverse legal profession that is more representative of the community that it serves, with arrangements more accommodating to childcare or other care responsibilities, or more accessible facilities for lawyers with disabilities.
- Reduced costs for the taxpayer, and with that the ability to support other parts of the justice system.
- A more positive emotional experience of the judicial process and a less intimidating atmosphere, which in turn can lead to more accurate decision making. For some parties or witnesses, being in the same room with the other party can be intimidating and effect their behaviour detrimentally.

With the experience from the COVID-19 years now available, a rigorous quantitative evaluation of the risks and benefits, and the impact they had on sentencing and decision patterns, is now both possible and necessary. Considering the impact that COVID-19 has had on the composition of cases that were decided (e.g. prioritisation of more serious cases, drop in some offences etc.), have there been statistically significant changes in decision patterns?

Secondly, how was the quality of the interaction with the justice system perceived by the participants? First evaluations indicate that professional lawyers were overwhelmingly positive about online hearings on more technical and procedural levels. On the other hand, there are reports of citizens who found the experience highly distressing and undignified – for instance hearing over a weak connection in a family court case the fate of one's children decided, without the emotional support a physical environment would have provided.

Even if, as the data seems to indicate, the experience was overall positive and few of the previous concerns materialised, the rule of law ideal requires that any future use outside an emergency context happen within a formal system of legal rules. These rules must be applied consistently, and provide appropriate remedies and avenues for appeal and redress in situations where the technology fails. If an online hearing is from an access to justice perspective helpful for one party, but disadvantageous for another, clear rules are needed to resolve conflicts.

While considerable discretion by the presiding judge might ultimately be necessary, these too need to be grounded in more general legal and ethical rules.

The digital infrastructure necessary for online proceedings that adhere to the rule of law will involve significant design decisions that are value-laden. This includes minimising inherent unfairness to or exclusion of users with less advanced technology, from bandwidth to processing speed of their devises. Similarly, the affordances of the digital court (e.g. how much help ambient AI provides to less legally skilled users, and how 'forgiving' the system is towards user mistakes) raise deep questions about procedural fairness and inclusion, decisions that can't be left to commercial software developers at all, as they touch upon the very core of the notion of a state under the rule of law, and require full and open debate.

How is 'Digital by Default' Widening Existing Social Inequalities?

The COVID-19 pandemic has shown some of the real consequences of being digitally excluded. As the nation went into lockdown, online services became the only option for some of the most basic activities. Work meetings turned into online conference calls, classrooms turned into online learning spaces and even social gatherings were carried out via some form of online connectivity. Having to rely so heavily on digital devices during this time has painted a stark picture of the impacts of digital exclusion – exacerbating the isolation and increased inequalities felt by those who are not digitally active. A lack of digital access has a social cost[13].

A common assumption is that the main demographic that suffers from digital exclusion is the older population, because they have not grown up with digital technologies, it was not part of their working life, affordability and lack of support. However, many factors can act as barriers to digital access across a wide range of demographics. Some of these include:

- Disposable income – can I afford broadband and appropriate devices?
- Competency – do I have the skills to engage with confidence?
- Disability – are digital tools and spaces designed with accessibility requirements in mind?
- Competency in English as a written language – are there inclusive options for non-English speakers?
- Access to reliable data and broadband (due to geography) – is there good coverage in my area that allows me to interact online?
- Education – do I have an awareness and understanding of the importance of digital engagement?

Often those who require digital access the most are the ones that struggle to find it. Not only can digital exclusion have a negative impact on wellbeing, but it can also mean that people may miss out on important information and opportunities. The Internet is becoming the key way to engage with vital establishments, including the government, local authorities, banks and many more. If digital inclusion is not addressed, people may suffer from:

- Fewer employment opportunities Less access to education
- Being information poor
- Not able to access necessary services
- Having to pay more for goods and services[14] (Snook, 2019).

[13] Digital Inclusion Synthesis report, Snook 2019
[14] Digital Inclusion Synthesis report, Snook 2019

It is clear that digital inclusion is not just about technology. Geography, background or ability should not be a barrier to successfully getting online. To ensure that everyone is able to access the benefits of a digital society, there are a number of key issues that should be addressed which can help everyone get online and have the confidence to engage.

The National Digital Ethics Public Panel Insight Report (2021) highlighted three priority areas where citizens felt that action is needed to achieve a digitally inclusive Scotland.

These are:

- Ensuring **fair and equitable** access to affordable digital technology and data
- **Removing barriers** so that all of the population are able to access skills and development opportunities that will enable them to participate online safely, productively and with confidence
- Ensuring that those who are not digital skilled (or choose not to engage digitally) are still able to access services that are provided as 'digital by default' without being disadvantaged.

> **" It's all very well to be told, "You can access that information online", but if I can't get decent broadband where I live, how does that help me? "**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 20**

Ethical Limits to Monitoring and Surveillance

Objects of Trust:

Technology: Is it reliable? Is it robust? Is it safe?

Privacy: Is my information confidential? Are there Laws/ Regulations to protect me? Are they being enforced?

Transparency: are the people behind it being truthful? Are there other motives?

What are Ethical Limits to Monitoring and Surveillance?

Monitoring involves either active or passive observation of an entity – whether this is a person, place or process. When we talk about surveillance, this can mean extended observation of a defined area or phenomenon, but, more negatively, it can also mean targeted monitoring specifically tracking movements, actions and interactions of people. The most problematic forms of surveillance can be untargeted bulk surveillance that is not driven by a specific suspicion or based on a concrete risk.

Monitoring and surveillance technologies can provide benefits to both the individual and society. For example, CCTV footage can be used in court as evidence to prove someone was in a certain place, or GPS mapping and tracking tools can help with navigation. However, in recent years monitoring and surveillance technology has started to become more pervasive and invasive, often in ways that individuals are unaware of. We have seen a rise in the use of facial recognition technology, and particularly during the pandemic, workplace monitoring. This raises serious concerns not only about the accuracy of the technology, but also about its proportionate use. Furthermore, it can question trusted relationships between individuals and organisations or employees and employers.

> **“ It has both pros and cons. I don’t like the idea of someone knowing where I am, it takes away some privacy. However, on the other hand, it could prove useful when members of the public aren’t following rules. ”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 56**

Why are Ethical Limits to Monitoring and Surveillance Important?

Monitoring and surveillance are already prominent and broadly accepted concepts in our society. However, as technology continues to provide new ways of embedding monitoring and surveillance into our daily interactions and activities, it can be more difficult to draw the line between what is acceptable, and unacceptable. Digital surveillance includes physical monitoring and tracking, such as tracking cars and automated CCTV systems – as well as monitoring in the digital space too, like online shopping habits or parents monitoring their children's phone usage.

New technologies have enabled more invasive surveillance in the workplace. We have seen examples of 'micro-management' through the use of keystroke counting or screen time monitoring, which has left people feeling demotivated and under pressure to be constantly online and working (National Digital Ethics Public Panel Insight Report, 2021). Collecting data in this way can often feel like it is monitoring without good reason, can suppress productivity and has the potential to breach privacy and data protection laws. This may erode trust in workplace relationships, where employees no longer feel that they have any autonomy over their own activities and workloads. If the data collected in these cases is not useful, and the technology is not being used in a targeted way, then it would seem that it is being deployed merely because it is there and available, rather than for a clear and proportionate reason. Limits, determined through public debate, around the use of monitoring and surveillance technology will help to ensure that its use is not intrusive, manipulative and unnecessary. Additionally strengthening regulation, legislation and oversight are levers available to mitigate the concerns on this evolving topic.

> **“ Problems could arise when data is collected and used for reasons not laid out and that is where it becomes unacceptable ”**
>
> **National Digital Ethics Public Panel Insight Report, 2021, P. 56**

Another example of digital monitoring and surveillance is the physical surveillance of public movements. Widespread anonymised data can be collected to help inform community level strategies for issues such as crime-prevention, public health or environmental planning and protection. However, often this is carried out in ways, which are not transparent or publicly understood. For this type of activity to be deemed acceptable, it is important that organisations communicate clearly, why there is a need to collect this data, and how the technology will be used to achieve this.

Additionally the practice of monitoring and collecting online data – dataveillance – such as monitoring credit card transactions, social networks, emails etc. creates a digital footprint of an individual's activity. While, again, there can be benefits to dataveillance, such as tracking fraud, there are a number of concerns around the practice too. People are not often aware that this type of surveillance is happening, highlighting a lack of transparency. Dataveillance can also compromise online anonymity.

Highly invasive and intrusive levels of surveillance cannot become the norm. There needs to be a balance – what can we deploy that is useful and proportionate and helps to keep society safe and flourishing; and how can we better limit, monitor and scrutinise surveillance technology and data collection so that it is used in ways that are fair, safe and transparent?

Privacy by Design and Default

High levels of surveillance and monitoring can be a violation of personal privacy. Privacy includes control over one's personal data and the spaces we occupy (physical or digital), from intrusion by public bodies, private organisations, employers and even within the family. Privacy is intimately linked to the concept of 'dignity'. Some level of privacy protection is provided by law, but there are many exceptions, and in some areas, such as rights of teenagers to privacy from their parents, there is little social consensus. There is a clear need to make sure that a digitally inclusive society can be achieved without citizens needing to worry about their safety and privacy in digital or physical spaces. Greater levels of transparency and awareness of the variety of methods of digital monitoring, and how monitoring can be controlled, and help to build public trust in the systems that people need to engage with.

Protection of individual privacy is a priority in the ethical deployment of monitoring and surveillance technology. Without citizens feeling confident that their data is safe, it will become increasingly difficult to maintain a sustainable relationship between public trust and the use of data-driven technologies.

To ensure that personal privacy is protected as far as possible, there is a need to establish ethical limits on the use of surveillance and monitoring technologies by:

- Ensuring there is no unfair use of monitoring that would invade personal privacy, by only using surveillance technologies with compelling reason and oversight
- Restricting the use of surveillance and monitoring technologies until they can be independently verified to meet high standards of effectiveness and accuracy, to be subject to proper governance, to address equality issues and to address authoritarian uses
- Additionally, the following principles, currently protected as legal rights under the GDPR need to be protected under any successor legislation, as without these principles a significant degree of data collection and processing could not be carried out in an ethically sound manner: Minimising the amount of information people are expected to provide when accessing goods and services
- Building privacy by design into apps and services as standard
- Providing the highest level of privacy settings as the default option
- Providing and inclusive broadband and mobile infrastructure.

Case study >

Case Study:

Cybersecurity

Dr. Markus Christen

Cybersecurity is a major area of growth and investment in Scotland, and the Scottish Government has been proudly promoting this sector as an enabler of prosperity and jobs.

The development of tools for strengthening personal and corporate privacy-protection, building cyber-resilience against threats presented by criminal or state actors, supporting financial or supply chain accountability and helping to tackle serious crime may, on the one hand be regarded as an ethical duty.

At the same time, the cybersecurity sector is also heavily investing in the development of surveillance and forensic tools for purposes such as law enforcement, border control, national security and behavioural monitoring, which can challenge public expectations for ethical, proportionate, transparent, fair, inclusive and accountable digital practice.

Investments in Scottish cybersecurity/forensics companies are partly based on the prospect of selling such technologies/services abroad. Some of these may be regarded as ethical exports, since they may help to guard vital public services or secure the assets and private information of citizens globally. Yet even the most well-intentioned technologies may be misused in the wrong hands; for example, there has been much coverage of Israel’s success in cybersecurity innovations, yet we are seeing evidence of these being used in domestic, corporate and governmental spyware, including by authoritarian governments or geopolitical adversaries of the UK. Scotland can make the most of a cyber-Scotland and avoid the potentially harmful effects of misuse and misappropriation by following three layers of action:

Government and legal: obtain an overview of the often-fragmented legal landscape, including gaps and conflicts, across the legislation areas of network and information security measures, electronic communications, including privacy and data protection issues and cybercrime.

Guidelines and soft law: Legislation will not be able to cover all cases/issues that will emerge in real life. Thus, what is needed is that companies themselves create a culture of awareness for such ethical and legal issues including procedures for how to operate (and deliberate) in case of unclear legal guidance. The process of generating guidelines within a company could be an instrument to enforce such a cultural change. Training of professionals on all levels:

It is well known that cybersecurity is a 'wicked problem' that cannot be solved but only be managed. Thus, knowledge regarding cybersecurity should include a broad spectrum of competences (certainly with a specified focus depending on the profession). What we consider relevant is that ethical, legal and social aspects of cybersecurity should be part of the training of professionals

Case Study:

Domestic Abuse and Data and Digital Technologies

Dr. Katherine O’Keefe

The use of digital technologies to facilitate domestic abuse mirrors many of the concerns revealed in the Public Panel about surveillance and technology. The increasing integration of digital connected devices into the home life impacts privacy generally but is of particular concern in the context of domestic abuse or intimate partner violence. Where the legal and ethical frameworks often used to raise concern regarding the impacts of digital technologies and surveillance on our rights to privacy, autonomy often model the threats and harms as external to the home and look for protection of the home from government, industry, or external criminal threats, the same threats to privacy, dignity, and autonomy can occur within the domestic space, in the context of intimate partner violence. This is reflected in the focus of legal protections. The UK Data Protection Acts and GDPR limit the scope of protections, exempting 'domestic' or 'household' use of personal data from requirements for compliance.

The impact of domestic abuse in Scottish life is wide-ranging and significant. According to research done by the Scottish Government 62,907 incidents of domestic abuse recorded by the police in 2019/20,[15] and the Coronavirus crisis saw a 'shadow pandemic', with an increase in reported domestic violence as well as increased threats and pandemic specific tactics of abuse during lockdowns.[16] “Some services observed increases in online stalking and harassment behaviours.”[17] According to Scottish Women’s Aid, “For women not living with their abuser, lockdown meant that their abuser knew they would be at home, increasing the abuser’s opportunities for stalking and continued harassment. The reliance on technology during lockdown to maintain social contact and for work also provided opportunities for abusers to misuse that technology to continue the abuse.” [18]

Many emerging digital devices and connected services have been weaponized by abusers as tools for surveillance or stalking (facilitated by GPS, webcams, spyware, or abusive uses of apps and phone functions), as well as control of 'smart' home IoT technologies such as smart meters, voice assistants, and locks. These can impact victims’ autonomy and be used as methods of coercive control and psychological abuse, to establish power over victims and harass them as well as for surveillance.

[15] Scottish Government (2021) Domestic abuse: statistics recorded by the police in Scotland - 2019/20 https://www.gov.scot/isbn/9781802010312

[16] O’Hare, Paul. “COVID in Scotland: What impact has lockdown had on crime?” https://www.bbc.com/news/uk-scotland-54342312

[17] Scottish Government (2020) ‘Domestic abuse and other forms of violence against women and girls (VAWG) during COVID-19 lockdown for the period 30/3/20 - 22/05/20’. https://www.gov.scot/isbn/9781839608292 Scottish Government (2020) Coronavirus (COVID-19): domestic abuse and other forms of violence against women and girls during Phases 1, 2 and 3 of Scotland’s route map (22 May to 11 August 2020) https://www.gov.scot/isbn/9781800040786

[18] Scottish Womens’ Aid (2021). Crisis and Resilience: The Impact of a Global Pandemic on Domestic Abuse Survivors and Service Providers in Scotland. https://womensaid.scot/wp-content/uploads/2020/09/SWA-COVID-Report.pdf

Technology facilitated abuse in the context of domestic abuse or gender-based violence is not necessarily fully recognized in the way domestic violence is recorded and countered in the justice system, though they are likely to fit into categories of "threatening or abusive behaviour or stalking" offences that constitute 88% of breach of the peace-type convictions recorded against abusers in the statistics recorded by the police in Scotland - 2018/19 (5). Additionally, the types of harassing and coercive behaviour for such digital abuse is intended to "cause the partner or ex-partner to suffer physical or psychological harm" such as fear, alarm, or distress. This is recognized in The Abusive Behaviour and Sexual Harm (Scotland) Act 2016 as an aggravation of an offense (Abusive Behaviour and Sexual Harm (Scotland) Act 2016, 1 (2)).

The harms of technology-facilitated abuse are significant, and part of a range of tactics used by perpetrators.

Restriction of access and monitoring of mobile phones has become a significant element of coercive control, as well as stalking behaviour. Abusers may misuse general-purpose software or operating system features or install more purpose specific spyware on phones. This can include changing passwords to block or control access to communications, as well as access to bank accounts and monitoring finances, using location tracking to surveil or stalk victim-survivors, and enabling spyware on phones. One example of psychological abuse often employed against survivors is harassment using payment apps, by repeatedly sending small payment amounts to constantly remind victims and survivors that they are within the abuser's reach.

Technology facilitated abuse, particularly in the context of smartphones and 'smart home' connected devices and systems integrated into the functioning of a home, raises specific privacy and security concerns for such sensitive situations and introduces new threats and harms. A number of digital technologies may be used by abusers as surveillance mechanisms to stalk victims and monitor their activity throughout the day as a tool of coercive control. This surveillance affects victims/survivors psychologically, impacting their dignity, privacy, and autonomy. The Scottish Government's reported that a commonly used phrase victims used was that they felt like "sitting ducks", as their abusers knew where they were at all times"[19].

This can include many 'internet of things' (IoT) devices as well as mobile phones. Webcams and home assistants, such as Alexa or Google Home devices, may be used for surveillance, or to control connected thermostats, lights, locks, and other elements of the home, connected devices, or wearables. The effects of this weaponized use are not only limited to the possible physical effects of the literal updated 'gaslighting', but the psychological effects of the threat whether the threatened control is possible or realized.

[19] Scottish Government (Jun. 2020). Coronavirus (COVID-19): domestic abuse and other forms of violence against women and girls - 30/3/20-22/05/20 https://www.gov.scot/isbn/9781839608292

There has been increasing recognition of the harm caused by non-consensual publishing of intimate images or 'revenge porn' as abuse and harassment. It is one of a number threatening and abusive uses of social media. The design of social media networks makes it difficult for abuse survivors to control their privacy and cut their abusers off from information about them, as their privacy is impacted by the social media profile privacy settings of everyone they know. Even if they block an abuser from all of their social media, they cannot ensure that everyone in their network also blocks information about them. Technologies such as facial recognition and automated tagging aggravate this risk.

At a government and policy level, support for the programmes and organisations working with victims and survivors of domestic abuse and gender based violence should consider the digital and physical abuse holistically. Similarly, the framing of legal protections in relation to data could take into account the gaps in protections resulting from 'domestic use' exemptions to data protection legislation. Support offering specialized expertise and cyber security support for survivors will likely be increasingly needed. Having a centralized government cybersecurity resource devoted to this, perhaps as an aspect of the Scottish cyber strategy, would also provide insight and statistics into the prevalence and trends in technology-facilitated abuse. Additionally, policies supporting better understanding of threats through Higher Education could offer another opportunity to help emerging developers understand the social context in which their products will affect people, individually and socially.

The Future of Work in a Digital Economy

Objects of Trust

Freedom of choice: Is it optional? Would not using it prevent me from doing important things?

Fairness: Is it accessible and usable by everyone who could benefit? Is it exploitative?

Institutions: Are they on the ball? Where does the buck stop?

What is the Future of Work in a Digital Economy?

"New industries appearing in this sector are great for employment and could involve retraining those in environmentally harmful industries for new work" (National Digital Ethics Public Panel Insight Report, 2021, p. 69).

The growth and advancement of digital technology and innovation is a priority for Scotland. With the ambition to become the 'data capital of Europe'[20] there is a drive to think about how businesses and organisations can start to adopt new digital tools and ways of working.

This means that the future of work will look slightly different. As has already been evidenced with the need for remote working over the COVID-19 pandemic, there is likely to be a shift towards remote working, using automated and cloud based services and relying more on digital tools to help support workers. The increased use of digital technologies could lead to a wide range of economic and social benefits.

Scotland's thriving technology sector could provide numerous economic impacts and opportunities for Scottish citizens. An increased focus on digital could deliver:

- Improved health and wellbeing
- Medical/safety advances
- Improved job quality
- Lower costs for consumers
- Potential for higher paid jobs
- Ease of communication with companies
- Convenience
- Greater consumer choice
- Access for people otherwise excluded from the labour market– disabled, carers, older people.

[20] Data-Driven Innovation (ac.uk)

> “ What are people are going to be re-trained to? Are there sufficient options and will there be the commitment and investment to back it up? ”
>
> National Digital Ethics Public Panel Insight Report, 2021, P. 68

Why is the Future of Work in a Digital Economy Important?

Scotland’s Digital Strategy (2021) outlines that "the businesses that have responded best to the challenges of the pandemic are those who have been able to innovate: pivoting quickly to homeworking, adopting cloud computing for speed and collaborative working, using new and secure digital platforms to access customers and to repurpose or diversify products and services and there is a growing body of evidence to suggest that this way of working is here to stay."

Whilst increased use of digital and automated services can help to offer an improved worker experience, there is a widespread concern that automation could lead to significant job losses and decreased social interaction. It may also exacerbate existing societal inequalities.

The balance between economic and societal prosperity is important when considering the future of work. Advancements in digital and AI technologies should be focused on assisting with human tasks, rather than eliminating them. Coupling this with investment in reskilling and the creation of new jobs in the digital sector will help to prevent largescale unemployment, as well as ensuring the workforce is appropriately skilled for the opportunities of the new market.

Case Study:

Governing the Rise in the Remote Economy

Sam Brakarsh & Prof. Abigail Marks

The Digital Strategy for Scotland (2021) sets as a goal that the country becomes a centre for home working, saying, “We will engage with communities in remote and rural areas to find ways in which Scotland can capitalise on changes in the world of work and position itself as a leading centre for home and remote working.” The articulated value of such an initiative is clear. It has the potential to increase the ease of work for entrepreneurs who would benefit from collaborations that extend beyond the local. Technologies exist to allow teams to coordinate without shared office spaces thereby purportedly increasing worker efficiency without in situ managerial supervision. In addition, remote work is framed as a solution to spatial inequality, opening up access to specialised employment for individuals in remote areas of Scotland who would otherwise find such opportunities restricted to those in larger cities and business centres. The potential for these benefits holds true. However, an overemphasis on remote work can lead to collective social harm and psychological harm. Comprehensive policy is needed to secure the economic and social gains whilst protecting against potential drivers of inequity that are embedded within remote work.

The language of inequality reduction can be co-opted by the for-profit industry to justify actions that may benefit the employer rather than the employee. Remote work can increase access to opportunity, but remote work is just as capable of being used as a strategy to shift costs of supplies and overheads onto employees. Throughout the COVID-19 pandemic, large organisations have provided insufficient support to employees to work from home. Most individuals have had to pay for basic office supplies out of pocket to make their home environment workable.

At least a quarter of employees had to finance provision for IT tools in order to homework during the COVID-19 pandemic and over half had to provide their own office equipment. In addition, working remotely is likely to silo employees and make collective mobilisation around worker rights more challenging. Shared hardships in the workspace are veiled through restricted social engagements on digital platforms. As one participant from the Working@Home project noted "And with the technology, you know, you can see people, talk to people… I think you missed some of the contact with people you’re particularly friendly with … So, there’s probably been occasions where it would be nice if, you know, we could get together." Asking the question of who remote work serves, the employee or the corporation, is vital in assessing how to protect the wellbeing and rights of Scottish peoples in the digital economy.

Remote work has its own barriers to entry. Blue-collar workers, whose labour is inextricably tied to their bodies, or those who work in Scotland's extensive tourist industry, will not benefit from policies aimed at increasing remote work. From a recent TUC (2021[21]) survey of employers, there is the suggestion that organisations are less likely to offer flexible work to staff who were unable to work from home during the pandemic. One in six (16 percent) of employers surveyed said that after the pandemic, they will not offer flexible working opportunities to staff who could not work from home during the pandemic, compared to one in sixteen (6 percent) saying they will not offer flexible working opportunities to those who worked from home during the pandemic.

We cannot allow flexible working to become a perk for the favoured few – offered to a minority of the workforce who are able to work from home – and serving to reinforce existing inequalities. The remote economy is most likely to support middle to upper-income workers whose skills are easily transferable to digital platforms. Remote work is not radically restructuring the economy. It removes some barriers to entry but introduces others. In particular, the Working@Home[22] project found that those who had large homes with less occupancy (and thus the space to afford a dedicated office) were more likely to 'succeed' at homeworking. From the Working@Home survey, it was clear that this advantaged men with 60% of men having a dedicated home office space compared to 49% of women. Moreover, with many remote workers having to pay for some of their own office equipment and IT provision, there is another advantage to those that are most affluent.

To find out more detail on Governing the Rise in the Remote Economy, **click here** to read the full case study from Sam Brakarsh & Abigail Marks.

21. Working@Home (org.uk)
22. Making Flexible Working The Default TUC Report 202

Balancing cultural enrichment, economic benefit and the environment

Having access to Scotland's shared cultural heritage such as; census records; birth, marriage and deaths records; world-leading collections in galleries and museums; and Scotland's treasures that are digitised in libraries, is a crucial part of building an ethical society. Through understanding our past, we can understand more about our humanity. Digital provides us a new way of accessing this past, and we must ensure that access to our digitised past is accessible by all. There are complex intersections between digital collections and social media platforms, and different values that come in to play when supporting digital infrastructures that are for cultural engagement, and wellbeing, that extend beyond the cultural and creative economy.

Beyond accessibility, emerging technologies can enable the generation of much-needed revenue for artists, as well as cultural organisations, which are currently heavily reliant on public funding. Last year saw the meteoric rise of Non-Fungible Tokens (NFTs), a blockchain-based, fundraising medium that introduced scarcity into the digital realm. NFTs are described as the digital-equivalent of limited editions (as visualised in Figure 2 of the linked case study) and sales in 2022 have already exceeded 37 billion US dollars (Chainalysis 2022). Having emerged in the aftermath of the pandemic, in early 2021, NFTs were deemed as a "lifeline" for "cash-strapped" cultural heritage organisations (Ciecko 2021). Indicatively, in 2020, Museums Galleries Scotland had reported that two thirds of the country's independent museums did not have enough funds to survive for a year (Knott 2020). With museums eager to explore new revenue streams, leading institutions globally experimented with NFTs; from the Uffizi Gallery in Florence to the British Museum in the UK. However, early experimentation from institutions with limited technological expertise, with a medium for which little is known, was bound to spark controversy and raise critical issues, as analysed in the attached case study. In addition, funding for cultural heritage, and digital cultural heritage, needs not to be only raised by institutions themselves: a society, which values its heritage and its past must fund its Gallery, Libraries, Archives and Museum (GLAM) organisations, and that includes providing adequate funding for them to embrace the opportunities and possibilities of digital.

Despite this, there are opportunities for the GLAM sector to experiment with new technologies. Even though there is currently a bear market within the crypto economy, more than 10 million US dollars are invested in NFTs every day (Anon. 2022c), highlighting the potential of this new fundraising medium, which has also opened up significant opportunities for artists and individual creators. Notably, Scotland is home to some of the world's leading figures of the NFT market. However, as a nascent medium, NFTs are plagued by risks and unknowns, such as the environmental impact of making and selling NFTs (depending on the underlying blockchain), the unclear copyright landscape, as well as the issue of digital deaccessioning. As NFTs present a form of ownership, publicly funded museums should be discouraged from selling NFTs of 'digital twins' of artefacts in their collections. These challenges persist and must be acknowledged and proactively addressed, as explained in the attached case study.

With £230 million being invested every year in Scotland's culture, historic environment and major events in order to ensure that the country's "world class cultural scene and rich heritage continues to thrive" (Dickie 2022) it is important to explore ways emerging technologies could make a substantial economic contribution towards that goal.

Given the potential of NFTs as a powerful fundraising medium, which could contribute towards the financial sustainability of individual creators and cultural institutions heavily relying on public funding, it is recommended for the appropriate framework to be provided, to enable interested parties to explore this new medium cautiously and methodically. Scotland is home to pioneers in the broader field of NFTs, from the world-leading Blockchain Technology Laboratory of the University of Edinburgh, which is pioneering developments in its field, to best-selling artists globally in the NFT market. Therefore, facilitating knowledge exchange between those pioneers to share their knowledge, insight and learnings with other fellow artists, researchers, as well as, creators, cultural institutions and innovation entrepreneurs, would help artists and heritage organisations start leveraging and eventually reaping the economic benefits of this new medium. More importantly, it will help form and foster a vivid community of creatives, researchers, practitioners and organisations that could make a major impact by helping shape the future of the rapidly expanding decentralised web. Funding and support for digital experimentation within the GLAM sector is crucial be able to make the most of our shared heritage, and to be able to build upon it. NFTs are just one example of the type of innovation that can occur in this space.

To find out more detail on NFTs and Cultural Heritage, **click here** to read the full case study from Foteini Valeonti & Melissa Terras. It should be noted that there are serious concerns over the use of NFTs and blockchain and their environmental footprint. This case study aims to profile the existence of a rapidly emerging technology in a sector less commonly associated with digital. This does not detract from the importance of understanding e-waste, per the other content of this report in the 'Green' Digital Scotland chapter.

How is the Digital Economy an Investment in our Collective Future?

A profitable economy can have a positive influence on a number of societal factors. However, it is important to balance this with an awareness of how a digital economy promotes fairness and inclusion. There is a concern that the push to digital will come at a disadvantage to those in lower paid or lower skilled roles. Whilst efficiency and automation can be useful, human flourishing should be the priority. That is why an Ethical Digital Nation must consider the impact of a digital economy on:

- Job losses
- The loss of human interaction
- Impacts on vulnerable groups
- Risks to safety of individuals
- Harms to employee rights
- Unequal access to Information
- Technology and digital skills
- Consumer Rights
- Education
- Climate and sustainability.

Case Study

Datafication of Higher Education

Joanna Van Der Merwe, Melissa Amorós-Lark, And Grégory Von Boetticher

Digital technology is being integrated into higher education at an exponential rate, especially as the COVID-19 pandemic moved teaching online causing severe educational disruption across the globe. If done correctly, these tools and data can change the way higher education is delivered, ensuring that it is flexible and accessible. It can also empower students and teachers by giving them insights into their learning and teaching practices allowing them to improve themselves and their learning/teaching journey. As well as using digital technologies to increase community engagement and participation. Conversely, if implemented without adequate ethical considerations this data can be used to create a model of education reliant on the constant surveillance of teachers and students rather than empowerment. Additionally, with data being used for profit motives, rights to privacy may be at risk and boundaries between personal and professional/student life blurred.

This case study takes on two examples to illustrate the ethical issues involving technologies, namely digital proctoring and the video-conferencing platform Zoom, which are currently in use and have permeated the (digital) education sector. Given the datafication of education, reflecting on the ethical concerns raised with existing technologies is vital in assessing the risks and benefits involved in future technologies and the design of a national policy on digital ethics.

Moreover, this case study contains insights from direct stakeholders such professors, student representatives and more. They touch upon themes such as awareness, data and digital literacy, the need to rethink education, new divides and barriers, funding, and power dynamics between institutions, staff, and students.

To find out more about the datafication of higher education in Scotland **click here** to read the full case study from Joanna van der Merwe, Melissa Amorós-Lark, and Grégory von Boetticher from Centre for Innovation Leiden University.

Case Study:

Fintech in Scotland

Felix Honecker

Over the past decade, innovations in financial technology (fintech) have started to transform the way financial services are delivered. Advancements in cutting-edge technologies such as artificial intelligence, natural language processing, cloud computing, Application Programming Interfaces (API), and blockchain continue to change how businesses in the sector operate, collaborate, and transact with their customers, regulators, and other stakeholders. Additionally, Open Banking practices allow fintech companies to access vast amounts of previously unavailable data (including transaction data), enabling them to develop new products and services that are potentially better suited to the needs of consumers.

Fintech's economic potential is staggering and investment into the sector is booming, with venture capital funding in 2020 exceeding $4.1bn in the UK alone.[23] Globally, the sector is projected to reach a value of about $305bn in 2025 – growth that is fuelled mainly by consumers and small and medium-sized businesses turning to fintech for payments, financial management, and financing.[24] When promoting the fintech sector, businesses, NGOs and policy makers alike have highlighted not only its huge economic potential, but also its capacity to trigger positive social change. Fintech can improve the efficiency and reduce costs of the current financial system, extending financial services to previously unserved or underserved households. However, consumer experts have identified several obstacles that could reduce the positive social effects of fintech and, potentially, leave consumers worse off.

There is no doubt that fintech can play a key role in delivering some of the National Outcomes set by Scotland's National Performance Framework. Scotland is home to a fast-growing fintech sector that benefits from the country's historically strong financial services expertise, world-class universities and talent, and excellent business support ecosystem.[25] The Scottish cluster has positioned itself among the leading fintech destinations in the UK and the world, creating high- income, tech-based employment in the country's fintech cities Edinburgh, Glasgow, Aberdeen, Dundee, Stirling, and Perth.[26] Through an increase in remote work, current and future jobs in fintech are no longer restricted to these larger cities but open up opportunities for high-quality employment across Scotland. Moreover, companies across a varied range of sectors can adopt financial technology tools for payments, accounting, cash flow management, smart contracts, and other business functions to increase productivity. These developments, therefore, contribute to the Economy, International, and Fair Work and Business outcomes of the performance framework.[27]

[23] EY Report: UK FinTech: Moving mountains and moving mainstream (2020).
[24] Market Data Forecast: Global Fintech Market Research Report (2021).
[25] FinTech Scotland Website: Why Scotland (Accessed 23 August 2021).
[26] UK Government: Kalifa Review of UK Fintech (2021).
[27] National Performance Framework: National Outcomes (Accessed 20 August 2021).

Notwithstanding the aforementioned opportunities, there are several challenges emerging from increased fintech adoption. Social inclusion could be at risk if the ongoing COVID-19 pandemic accelerates the transition to digital financial services. Unequal access to digital infrastructure (e.g., lack of access to mobile phones, computers, or the internet) could exacerbate existing and create new forms of exclusion. Additionally, people who may have access to the necessary infrastructure but lack digital expertise may refrain from using new technologies and miss the opportunities associated with them. This could aggravate existing inequalities, expand the digital divide, and further isolate vulnerable groups.[28]

Similarly, machine learning and data biases (which occur due to prejudiced assumptions made during the algorithm development process or biased training data) as well as inaccurate or incomplete data could restrict rather than broaden access to credit. There is some evidence indicating that, instead of delivering on the promise of facilitating access to affordable credit for previously excluded consumers, increasing data points in credit scoring also increases inaccuracies which in turn negatively affect creditworthiness.[29] People who deliberately avoid leaving a data trail or who suffer from data poverty[30] will be disadvantaged by these approaches if there are no moderating measures in place.[31] This potentially forces people to establish a data history at the expense of their privacy if they want to avoid being subjected to unfair price discrimination (or being excluded from credit altogether). At worst, some of our most sensitive and private data could be extracted and used for exploitative ends. Thereby, the financial inclusion argument could be co-opted by firms to bolster their legitimacy.

[28] Finance Watch Report: A Wrinkle in the Process: Financial Inclusion Barriers in an Ageing Europe (2021).

[29] NCLC Report: Big Data, a Big Disappointment for Scoring Consumer Creditworthiness (2014); Oliver Wyman Report: Alternative Data and the Unbanked (2017)

[30] Nesta Innovation Policy Report: Data Poverty in Scotland and Wales (2021).

[31] Barclays Report: Open Banking – A Consumer Perspective (2017).

> “ There is more to being online than we realise. Seek knowledge so you are aware of the personal and societal impacts of what you are doing. ”
>
> National Digital Ethics Public Panel Insight Report, 2021, P. 74

Recommendations

Recommendations

What will an Ethical Digital Scotland look like?

The Expert Group recognises that digital ethics is an inclusive term covering a wide range of moral considerations involving digital products, services and methods that affect society. These are already being considered under banners such as computer ethics, internet ethics, data ethics, AI ethics and robot ethics, or as part of the 'tech for good', responsible innovation and digital inclusion movements, amongst others. Likewise, they are manifesting in widely diverse sectors using or affected by digital innovations, from the charitable and healthcare sectors to financial services and online gambling.

Key Issues:

Privacy, Transparency, Inclusion, Rights, Safety, Democracy Power, Accountability, Fairness, Engagement, Awareness, Investment, Support, Communication, Oversight

This report has aimed to capture, interpret and synthesise evidence and real-world knowledge about digital ethics challenges affecting Scotland (albeit many are universal issues), and to make recommendations to facilitate the government's aspirations for an Ethical Digital Nation, as laid out in the Programme for Government. The recommendations given will help steer the Scottish Government on how to enact these practically. These recommendations have been informed by the best available evidence, expert knowledge and insights from multiple publics and stakeholders. This paints a holistic picture of what an Ethical Digital Scotland will look like across all areas of society. It captures the hopes, expectations and concerns of the public and highlights how government, businesses, civil society groups and citizens can help to foster digital ethics and moderate harms.

Public trust should be at the forefront of all decision making regarding Scotland's status as an Ethical Digital Nation. Using the Objects of Trust Framework as a means of challenging and questioning new and emerging technologies, and utilising the framework's links to the National Performance Framework will allow for the measurement, tracking and monitoring of Scotland's journey to realising its ambition as an Ethical Digital Nation.

In order to become an Ethical Digital Nation, Scotland will need to pledge that all the economic benefits brought via digital will not be at the expense of ethical considerations. **A priority for government is to reconcile the need for top-down legislation, regulation, governance and enforcement with a large-scale push and promotion of education, awareness and upskilling campaigns throughout the nation**. These should be considered priority actions moving forward. Public awareness and understanding is critical to ensuring that organisations and governments can be held accountable for the deployment and use of digital technologies. Additionally, a stronger form of participatory governance in the digital sphere will ensure that decisions made about the people, are made with the people.

Recommendation Summary

Desire for a National Digital Guardian

Fractured responsibilities and lack of holistic oversight is leaving too many gaps in the governance of digital innovations by both the public and private sector. Where unethical or problematic practices are witnessed, too often it is unclear which of the plethora of regulatory or support agencies with their different remits, these issues should be raised to (e.g. advertising, consumer protection, data privacy, cybersecurity, policing etc.).

In addition to the presentation of recommendations thematically a requirement that was often mentioned in the Public Panel, is the need for a 'go-to' digital 'ombudsman'.

To support this recommendation, there is a need for a comprehensive overview of the laws and regulations that can be brought to bear in Scotland to ensure digital ethics, particularly in cases of online harm, as well as to understand the challenges that would be involved in aligning existing diverse bodies around a common set of digital governance objectives.

Securing Trust in Government Digital

Scotland is on a mission to be a world- leader in data-driven innovation, with bold plans to harness information about citizens, government, businesses, the economy and our natural environment, to serve various goals for science, society, and the econom Plans to digitise government services are also moving apace, with digital first systems, the data intelligence network and digital identity credentialing projects at an advanced stage.

- Ensure this is done with the consent or verified assent of all stakeholders.

Allegations of unfair procurement, unwise partnerships with Big Tech, wasteful spending and abuse of data power, levelled south of the border during COVID-19, have fuelled widespread public (including media) concern about integrity in public life.

- The rule of law and standards in public life must be seen to be adhered to through transparent and accountable government decision making and spending around technology projects, grants, contracts etc. Open Government (a coalition of active citizens and civil society organisations committed to making Scottish government work better for people) is part of this.

- Multiple strategies for involving citizens should be pursued, including information campaigns, and online surveys or consultations, to long- lasting deliberative engagement and direct participation in decision- making groups and institutions.

- Honest conversations about difficult trade-offs are needed, especially where digital decisions may cause harm to certain individuals or groups but may be 'fair' and necessary in other ways. A deeper understanding of the impact of digital innovation on the environment is also needed.

Presentation of recommendations thematically

Public Awareness of Data Use and Sharing & Harm Protection when Online

There is a strong need for actions to protect citizens from harms caused by malign online influences, particularly in the case of children. These involve both direct and indirect forms of harm, including:

- Industrial harms such as pornography, gambling, fast-food marketing
- Criminal harms such as grooming, blackmail, drug pushing
- Psychological harms, such as stalking, sexting, shaming, cancelling
- Group harms, such as racism
- Covert exploitation such as addictive media, product placement in online games, or auctioning the web clicks of identifiable users to advertisers
- Vulnerable groups (e.g. domestic violence victims may be digitally stalked but their privacy may also be abused during police investigations).

Tackling these many different forms of harm is no mean feat. As already noted, it can involve many different agencies and instruments and the sources and severity of harm can sometimes be hard to pin down. The major internet, social media, streaming and gaming platforms are headquartered overseas and the laws surrounding their obligations for consumer and data protection are reserved. This limits how much direct control the Scottish Government can exert over these practices. Many other steps are nevertheless possible. These include:

- Scottish MPs advocating for change in the UK parliament
- Scottish Government exerting soft influence through lobbying platforms for change
- Sponsorship of support agencies and helplines
- Appropriate information/education for different age groups aimed at raising awareness
- Due diligence to ensure Scottish Government is not inadvertently incentivising or sponsoring Scottish business that contributes to these harms
- Building on existing efforts on legal enforcement and prosecution, while taking into account the risks associated with surveillance and monitoring mentioned earlier in the report.

Scotland’s businesses, public sector and citizens are subject to harm from cybercrime – not only carried out by opportunists, but also organised crime groups and state actors. This can target infrastructure, money, intellectual property, or personal information. These actions can directly damage vital systems, livelihoods, reputations, services, political actors and the economy as a whole. Technologies are being designed to support cybersecurity, many in Scotland, but these can also lead to more intrusive surveillance of individuals and still holds the potential to be misused.

- Continued investment in cybersecurity capacity building is essential and, given the workforce shortage, it is inevitable that automated technologies will have to play a role. It is key that innovation is guided towards producing ethical technology that prioritises human rights, here or abroad.

There is potential for digital forms of engagement to enable democratic participation at a local, community, council or governmental level.

- Further work to establish the best way of leveraging digital engagement methods would be worthwhile, along with the resources to support this.

The internet and social media are seen as primary sources of misinformation and disinformation, although this can equally be disseminated via traditional media and public figures. All of which is weakening trust in institutions, undermining faith in democracy and polarising communities.

- Careful educational campaigns and better use of social media by independent democratic bodies is necessary to help overcome this
- Ethical use of methods such as social network analysis can help to expose patterns of political influence and may prove useful as an educational resource.

A ‘Green’ Digital Scotland

Scotland is leading the way in green tech, much of it digital, offering new opportunities to address the UN Sustainable Development Goals for climate action. As we strive to become a leading nation for big data, high performance computing, artificial intelligence, digital gaming, cryptocurrency and space technology, as well as ‘digital first’ public services and ID, there has been a failure to acknowledge the environmental cost. The power consumption of some of these innovations dwarfs that of many conventionally energy intensive industries, such as plane travel. Computers also create heat and storing files on the internet requires data to travel thousands of miles. Recycling facilities and repair opportunities are under-developed, leading to digital waste.

- Close coupling the data and digital innovations strategy with the renewables agenda is vital
- Develop a strategy for managing digital waste and sponsoring repair
- Keep Scottish e-waste in Scotland
- Invest in professional e-waste recycling units
- Mandate purchase of digital products that allow for repair and recycling
- Work with technology companies in Scotland to support efforts to reduce emissions.

Digital Inclusion

Access to digital technologies can reduce barriers to participation (e.g. supporting the disabled to work from home, enabling rural patients to receive healthcare). It can also perpetuate or even magnify existing disparities, both through affordability gaps or lack of empowerment and skills (e.g. participation in online finance.)

Digital technologies may also hinder some groups' ability to exercise their rights or freedoms, either 'by design' or as an unintended consequence. Using fully automated systems to calculate people's eligibility for services, likelihood of committing crimes, or ability to benefit from treatment may fail to recognise individual circumstances and have unfair outcomes. Certain technologies may be more unfair for specific groups (e.g., a Digital Identity may be convenient for many people but aversive to refugees with experience of their misuse). Use of broad-brush data mining or surveillance may unfairly stigmatise certain groups or compromise their rights (e.g. area- based labelling for health risks may impact insurance costs; facial recognition in shops violates privacy, stigmatizes the innocent and can subject people to unequal treatment by ethnicity and gender.)

- Actions are needed to anticipate and mitigate any risks of exacerbating the digital divide, when planning new government projects, as well as to flag non-governmental sources of digital inequality that may require intervention

- Ensure equal access to public and essential services is maintained by guaranteeing alternative options are always available, without this being a disadvantage in terms of cost, eligibility or quality

- Regulate pricing on network data provision

- Encourage businesses providing data, devices and software to take some responsibility to ensure access to their digital services is affordable and accessible to all consumers that go beyond the existing very basic responsibilities.

Reliable, Representative Data & Technologies Underpinning Algorithmic Decision Making

Both to build trust into algorithmic decisions and to comply with guidance in place in data protection laws, organisations need to be able to demonstrate that their algorithms are robust, reliable and meet a set of required standards. If the algorithm is determining whether someone can access education, buy a house or get a job, they need to feel confident that the outcome is justified. It is not just the outputs that need to be considered, but also how the algorithms are deployed.

- Algorithms should always be applied fairly and equitably, which is best done through human oversight and appropriate, potentially participatory, governance

- There should always be a way to determine how a decision was made.

Total transparency may not always be appropriate. Some companies may want to keep their algorithms secret to avoid competition, or sometimes the data used could be sensitive and personal, and information that warrants high levels of protection.

- Improve regulatory practices around transparency that will push companies to provide more accessible explanations of how their algorithms work
- Introduce external audits to provide an extra layer of scrutiny around algorithmic decision making that can reassure the public that agreed standards are being met
- Human 'sense check' to validate the decisions the algorithm is making.

Ethical Limits to Monitoring and Surveillance

Values can clash in the digital space. A company may desire the best tech to help their users, the police may wish the best surveillance cameras to help them protect the public, and a government may wish the best data to optimise public services. However, data over-reach, lack of consultation and consent can be seen as disproportionate, disrespectful and dishonest, damaging the public trust needed for success.

- Active involvement and lay consultation and participation are needed, especially for the most sensitive types of data mining or surveillance
- Transparent, inclusive and democratic engagement in strategic planning and decision-making to ensure a fair deal for data usage and calibrate uncomfortable realities
- Enforcement of legal duties around data protection and strong actions to minimise the use of person-level data and ensure anonymisation
- Development of ethical guidance around group privacy and demographic-level harms due to the gap in data protection law unable to adequately address the risks and harms related to use of aggregate data.

The Future of Work in a Digital Economy

A profitable economy can have a positive influence on a number of societal factors. However, it is important to balance this with an awareness of how a digital economy promotes fairness and inclusion. There is a concern that the push to digital will come at a disadvantage to those in lower paid or lower skilled roles. Whilst efficiency and automation can be useful, human flourishing should be the priority to guard against:

- Net Job losses
- Lack of human interaction
- Impacts on vulnerable groups
- Risks to safety of individuals
- Harms to employee rights
- Unequal access to digital technologies
- Lack of consumer rights.

As Scotland's homegrown tech sector thrives, much has been made of the new 'high value' jobs that are emerging but this affects a tiny minority of elite earners, with no guarantee of trickle-down.

- Track whether these lead to broader career paths to ensure this leads to wider scope of employment opportunities
- Provide appropriate and accessible upskilling opportunities to minimise net job losses caused by automation and other digital advances
- Support digital infrastructures that improve wellbeing and societal flourishing, such as cultural heritage.

New forms of employee monitoring are causing alarm due to a lack of transparency and a sense of over-reach and privacy violation. The use of data analytics may help businesses and some workers to understand performance better but could also affect their autonomy.

- Work with organisational leaders and unions to ensure clear and consensus-based policies
- Ensure surveillance and monitoring technologies are used in a controlled, transparent way
- Establish regular reviews of surveillance technologies to ensure their use is still justified and proportionate
- Develop and adopt codes of conduct that make a commitment to fair and ethical practices
- Need to work with the cultural, financial and environmental agenda to research this area further.

Annex

The following section and tables have been included as an annex for detailed recommendations under the thematic chapters

Public Awareness of Data Use and Sharing

Education and oversight are key levers when it comes to raising public awareness of data use and sharing. Government, business and civil society organisations all have responsibility to provide citizens with the knowledge and tools required to safely navigate the Internet and digital technology. Likewise, individuals themselves have a responsibility to take up these opportunities. In addition to this, it is recommended that Government strengthen its regulatory and legal controls concerning: its commitment to open data principles; the standards and principles around data use and data sharing; and independent oversight.

Recommendations	
Governments & Government Bodies	• Provide all citizens will the knowledge and tools to safely use and navigate the Internet and digital technology • Enable citizens to easily identify the ownership, and links between, social media and other web-based platforms • Invest in the relevant technical and legal mechanisms that will build public trust and awareness of data use and transparent • Commit to open data principles on government data • Commit to undertaking an audit of automated decision making Create a public register of all targeted advertising by government • Create an internal review board for digital behaviour change programmes undertaken by the government
Businesses	• Create education programmes to raise awareness with employees and customers on how to safely navigate the Internet and digital technology • Enable users to easily identify the ownership, and links between, social media and other web-based platforms • Provide clear and transparent explanations of how data is shared, used and stored, beyond regulatory requirements • Encourage a culture of awareness for ethical issues and to develop procedures to address how to operate and deliberate in the case of unclear legal guidance • Ethical, legal and social aspects of cybersecurity should be part of the training of professionals at all levels

Recommendations	
Society and Civil Society Organisations	• Raise awareness on how to safely navigate the Internet and digital technology • Participation in governance and decision-making by citizens and communities
Individuals	• Self-educate before providing sensitive data online

A ‘Green’ Digital Scotland

Once again, education is seen as a key driver to bring us closer to an ethical ‘green’ digital Scotland. This is a shared responsibility across government, business, civil society and individuals. Acknowledging both the advantages of digital innovation in move towards a more sustainable future and the environmental cost of digital will allow all responsible parties to strategise how they can make a difference in this domain. Beyond education, oversight also has its part to play from a policy point of view.

Recommendations	
Governments & Government Bodies	• Raise awareness of the negative climate impacts of digital with businesses and citizens • Invest in renewable energy digital infrastructures, e.g. by making sure new data centres are net-zero • Ensure a policy environment conducive to renewable energy installations Keep Scottish e-waste in Scotland • Invest in professional e-waste recycling units • Mandate purchase of digital products that allow for repair and recycling • Work with technology companies in Scotland to support efforts to reduce their emissions • Design and deliver a public awareness campaign of the potential climate risks associated with the use of technology, and how to mitigate these
Businesses	• Reduce the environmental impacts of digital use and the manufacture • Reduce energy consumption and/or invest in the generation of renewable energy • Favour low or zero-carbon digital services (cloud computing) • Minimise use of rare and virgin resources • Encourage purchase of digital products with the longest warranties • Encourage purchase of digital products whose design allows for repair and recycling (both for customers and internal operations) • Minimise irresponsible business practices that encourage addictive online behaviour

Recommendations	
Society and Civil Society Organisations	• Encourage the repair of digital devices • Encourage recycling of digital devices where appropriate
Individuals	• Minimise device upgrades until absolutely necessary • Ensure old devices are appropriately reused or recycled

Harm Protection when Online

It is essential that oversight is strengthened, and at pace, when trying to combat online harms. This includes creation of independent bodies for oversight purposes, implementation of regulatory standards, legislative steps and increasing policing powers. Communication is also key to enable international liaisons to tackle issues, to allow for transparency and to bring in the voice of the public for a better understanding of how to prevent these harms. Additionally governments and business alike must support individuals in both prevention and seeking redress, with clear reporting protocols in place.

Recommendations	
Governments & Government Bodies	• Establish independent oversight of digital data collection and use (nationally or internationally) that can be enforced against unethical practice • Liaise with international government bodies to ensure this framework can stretch beyond national borders, just like the technology • Help individuals seek redress from malicious and intentional harms • Impose regulatory standards that ensure greater transparency about the sources of information online in ways that are easy to verify • Investigate how stronger age verification checks for child safety could be implemented successfully, through legislation or other routes • Strengthen public and third sector resources to tackle online harms • Continue to support businesses in getting the basics of security and data management right

Recommendations	
Businesses	• Continue to invest in preventing online hacks and leaks • Help individuals seek redress from malicious and intentional harms • Ensure greater transparency about the sources of information online in ways that are easy to verify • Build in ethical controls on the development and implementation of advertising algorithms • Have clear and user-friendly reporting procedures for abuse/ harassment
Society and Civil Society Organisations	• Support individuals to develop skills to critically evaluate information and its sources, including fact checking and skills training • Acting on the collective responsibility of civil society on oversight and governance in the digital public sphere
Individuals	• Develop skills to critically evaluate information and its sources, on topics such as online bullying and cybersecurity

Reliable, Representative Data & Technologies Underpinning Algorithmic Decision Making

The weight of recommendations on building trust into algorithmic decision-making is around communication. Businesses and governments need to be able to demonstrate that their algorithms are robust, reliable and meet a set of required standards. Equally, communication is needed in the other direction from individuals and civil society on bad practices to apply pressure to organisations to improve their practices. Oversight is another key tool here, allowing for standards of transparency to be put in place and regulated over.

Recommendations	
Governments & Government Bodies	• Implement regulation over the use of unreliable and discriminatory technologies • Support the development of standards and ensure standards of transparency over algorithmic decision making are met • Provide routes for users to complain and seek redress

Recommendations	
Businesses	• Demonstrate that algorithms are robust and reliable using standards based and auditable processes • Make clear to users how their data is being used to make decisions about them • Ensure standards of transparency and accountability are met • Build in human validation and verification of outputs as standard to development of algorithms as standard to development of algorithms as standard to development of algorithms as standard to development of algorithms • Provide routes for users to complain and seek redress
Society and Civil Society Organisations	• Call out bad practice and put pressure on organisations to justify the legitimacy of their algorithm-based processes • Advocate for the necessity and then the fair and just use of algorithms in decision making processes • Facilitate participation in governance and decision-making by citizens and communities
Individuals	• Highlight and report failures and biases evident in the system • Be aware of the types of digital interface that could potentially be subject to bias • Support others in your family and social network

Digital Inclusion

Both education and support are critical to reducing the barriers to digital participation. Governments, civil society and individuals have to work in unison at bridging the divide in digital literacy, particularly to marginalised groups. Businesses also have a role in educating their employees but have a stronger part to play in providing support to their customers, in terms of ensuring that alternative options to digital are available and equitable.

Recommendations	
Governments & Government Bodies	• Champion initiatives to ensure that access to digital, data and technology is affordable • Regulate pricing on network data provision • Increase the speed and roll out of public education and awareness on the benefits of digital skills, and make sure that school, public and professional education is kept up to date in order to deal with constantly changing risks and opportunities. • Provide accessible education and training opportunities for digital upskilling

Recommendations	
Governments & Government Bodies	• Ensure that there is a governance framework to support public and private organisations to be meet standards, which require that equal access to public and essential services are maintained. Standards should guarantee that alternative options to digital are always available, without this being a disadvantage in terms of cost, eligibility or quality • Create a legal framework for the use of online courts that gives clear rules under which conditions the party can ask for online proceedings, or refuse to participate in online proceedings • Use the experience from the COVID-19 trial to develop an online court platform that ensues fairness to all parties when using it and mitigates biases created by the digital architecture
Businesses	• Businesses providing data, devices and software should take some responsibility to ensure access to their digital services is affordable and accessible to all consumers and that alternatives are provided, via enhanced statutory minimum accessibility requirements • Implement social corporate responsibility pledges that guarantee that basic (but functional) devices continue to be produced to ensure replacement and upgrade costs are not prohibitive (e.g. for mobile phones) • Promote digital inclusion internally by upskilling and training employees in digital skills, supporting employees to adapt to hybrid working • Ensure equal access to services is maintained by guaranteeing alternative options are always available, without this being a disadvantage in terms of cost, eligibility or quality
Society and Civil Society Organisation	• Invest in and organise hubs for the re-distribution of devices that are no longer required • Volunteer to train or teach others in the community, reflecting on previous learning from existing programmes • Build on community digital hubs already established
Individuals	• Raise awareness of the benefits of being digitally active, particularly in marginalised groups such as the elderly (poorer) • Take up digital opportunities where available and feel empowered to decline opportunities

Ethical Limits to Monitoring and Surveillance

Responsibilities with regards to limiting monitoring and surveillance can be segmented between governments and business needing to implement huge amounts of oversight in this area and civil society and individuals having a responsibility on the other end of this around education. At present regulation is scant in this sphere and escalating instances of abuses of power in this area show the need for swift action on implementing regulation. In the meantime, citizens need ways of becoming aware of the risks associated with monitoring and surveillance so that they are empowered to make appropriate choices in their daily lives.

Recommendations	
Governments & Government Bodies	• Ensure that regulators are keeping pace with, and anticipating, future digital developments • Ensure that measures of surveillance and monitoring that are necessary, proportionate and justified by compelling reasons • Establish an independent governance body or a specialist advocate for citizens to regulate any surveillance and monitoring of the general public, its justification and its proportionality. • Build public awareness of data collection and use of surveillance technologies • Ensure that regulations placed on technology companies are fair to their users and wider society, first and foremost, and then fair to the company • Ensure that surveillance and control does not overly affect the most disadvantaged, those on benefits etc.
Businesses	• Ensure surveillance and monitoring technologies are used in a controlled, transparent way • Establish regular reviews of surveillance technologies to ensure their use is still necessary and proportionate • Consult with governments to ensure there is a balance between regulation and service offerings • Develop and adopt codes of conduct that make a commitment to fair and ethical practices • Build privacy by design into apps and sites as default • Ensure highest privacy settings are enabled as the default option
Society and Civil Society Organisations	• Use ‘purchase power’ to demand better from service providers • Use public voice to ensure that greater levels of surveillance within society do not overstep public expectations
Individuals	• Use ‘purchase power’ to demand better from service providers • Contribute to discussions ensuring that greater levels of surveillance within society do not overstep public expectations

The Future of Work in a Digital Economy

Both support and education are required to ensure that the workforce is prepared for future developments in the digital economy. Governments and businesses both have a role in developing citizens, as employees, to face the future and that must be done in an accessible and inclusive way. Individuals then have a responsibility to make the most of these opportunities when presented with them.

Recommendations	
Governments & Government Bodies	• Maximise economic and development opportunities that digital can offer to Scotland • Minimise net job losses caused by automation and other digital advances Provide appropriate and accessible upskilling opportunities • Ensure the education system prepares students for new types of work in the future • Commit to supporting digital infrastructures that support wellbeing and societal flourishing, such as cultural heritage • Support the openly licensed digitisation of the past and providing access to this digitised content to all • Commission an in-depth investigation into non-fungible tokens
Businesses	• Maximise economic and development opportunities that digital can offer to Scotland • Minimise job losses caused by automation other digital advances • Manage the transition to digital by retraining and upskilling staff where appropriate
Society and Civil Society Organisations	• Encourage uptake of digital skills training where offered • Maximise community-driven development opportunities that digital can offer to Scotland
Individuals	• Engage in digital skills training opportunities

Bibliography

Digital Directorate. (2021, March 11). A changing nation: how Scotland will thrive in a digital world. Retrieved from gov.scot: https://www.gov.scot/publications/a-changing-nation-how-scotland-will-thrive-in-a-digital-world/

Jones, J. (2018, August 28). How Twitter Bots and Sock Puppets attack pro-independence women. Retrieved from The Herald: https://www.heraldscotland.com/opinion/16601876.twitter-bots-sock-puppets-attack-pro-independence-women/

Laville, S. (2019, February 7). UK worst offender in Europe for electroic waste exports - report. Retrieved from The Guardian: https://www.theguardian.com/environment/2019/feb/07/uk-worst-offender-in-europe-for-electronic-waste-exports-report

Leask, D. (2018, August 28). Meet the McBots: how Scottish cyber activists try to game Twitter. Retrieved from The Herald: https://www.heraldscotland.com/news/16601798.meet-mcbots-scottish-cyber-activists-try-game-twitter/

McLaughlin, M., & Andrews, K. (2020, November 30). Foreign interference undermining SNP, conference told. Retrieved from The Times: https://www.thetimes.co.uk/article/foreign-interference-undermining-snp-conference-told-0qdfd8hp7

Rossi, R & Nairn, A (2021, October 26) What Are The Odds? The Appeal of Gambling Adverts to Children and Young Persons on Twitter

Rossi, R et al. (2021, October) “Get a £10 Free Bet Every Week!” - Gambling Advertising on Twitter: Volume, Content, Followers, Engagement and Regulatory Compliance

Scotsman. (2018, August 23). ‘Facebook removes pro-Scottish independence page linked to Iran’. Retrieved from https://www.scotsman.com/news/politics/facebook-removes-pro-scottish-independence-page-linked-iran-1426569

Scott, K. (2021, September). National Digital Ethics Public Panel Insight Report. https://www.carnegieuktrust.org.uk/publications/national-digital-ethics-public-panel-insight-report/

Scottish Government. (2018, July 4). National Performance Framework: what it is. Retrieved from National Performance Framework: https://nationalperformance.gov.scot/what-it

Scottish Government. (2020, July 30). National Expert Group on Digital Ethics. Retrieved from gov.scot: https://www.gov.scot/groups/national-expert-group-on-digital-ethics/

Snook. (2019). Digital Inclusion Synthesis Report. https://wearesnook.com/our-principles-for-digital-inclusivity/

United Nations Department of Economic and Social Affairs. (2022). SDG Goal 16. Retrieved from Sustainable Development Goals: https://sdgs.un.org/goals/goal16

Wilcox, B. et al. (2005) Report of the APA Task Force on Advertising and Children

Attributions

Commissioning and Secretariat

Report commissioned by The Scottish Government from Edinburgh Innovations, University of Edinburgh

Secretariat provided by Digital Directorate, The Scottish Government

Editors

Alex Hutchison, Director of the Data for Children Collaborative, University of Edinburgh

Alessandra Fassio, Advocacy & Relations Manager, University of Edinburgh

Expert Group

Dr Claudia Pagliari, Digital Ethics Expert Group Chair, Senior Researcher and Director of Global eHealth, University of Edinburgh

Dr. Oliver Escobar, Senior Lecturer in Public Policy, Edinburgh Futures Institute, University of Edinburgh

Dr. William Huber, Centre Director, Head of Centre of Excellence, Abertay University

Dr. Katherine O'Keefe, Director of Training and Research, Ethicist, Castlebridge Consulting

Prof. Burkhard Schafer, Professor of Computational Legal Theory, University of Edinburgh

Dr. James Stewart, Lecturer, Science Technology and Innovation Studies, University of Edinburgh

Prof. Shannon Vallor, Baillie Gifford Chair in the Ethics of Data and Artificial Intelligence, University of Edinburgh

Prof. Alan Winfield, Professor of Robotic Ethics, University of the West of England

Research Assistant

Lizza Dauenhauer-Pendley (from April 2021 to November 2021)

Case Study Contributors

Melissa Amorós Lark, Project Lead, Centre for Innovation, Universiteit Leiden

Dr. Matthew Barr, Senior Lecturer, University of Glasgow

Grégory von Boetticher, Intern, Centre for Innovation, Universiteit Leiden

Sam Brakarsh, Early Stage Researcher, Oxford University

Dr. Ben Collier, Lecturer in Digital Methods, University of Edinburgh

Dr. Markus Christen, Managing Director of the UZH Digital Society Initiative, Universität Zürich

Dr. Laura Fogg-Rogers, Associate Professor, University of the West of England

Felix Honecker, Early Stage Researcher, University of Glasgow

Prof. Abigail Marks, Prof of Future of Work, Newcastle University

Joanna Van der Merwe, Senior Policy Advisor, Universiteit Leiden

Gerry McGovern, Founder & CEO, Customer Carewords, Author – World Wide Waste

Prof. Agnes Nairn, School of Economics, Finance and Management, University of Bristol

Dr. Raffaello Rossi, Lecturer in Marketing, School of Management, University of Bristol

Prof. Melissa Terras, Professor of Digital Cultural Heritage, University of Edinburgh

Dr. Foteini Valeonti, AHRC Innovation Leadership Fellow, Department of Information Studies, University College London

Building Trust in the Digital Era:
Achieving Scotland's Aspirations as an Ethical Digital Nation

Digital Ethics Expert Group Report

Scottish Government
Riaghaltas na h-Alba

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-80525-041-8 (web only)

Published by The Scottish Government, November 2022

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1171762 (11/22)