Socitm

Harnessing data:

Data ethics and acceptable use *BETA*

BETA version

The content in this section is available in a BETA version and is currently being reviewed.

Please send any comments and suggestions, additional resources and/or case studies that may help to improve or update this content to:

martin.ferguson@socitm.net

Data ethics and acceptable use

Data ethics has suddenly become a hot topic. Some of this comes from the GDPR initiative which has raised awareness and some from various data scandals (e.g. Cambridge Analytica), failed data projects (e.g. Care.Data) and cyber breaches (just to many to list!). There is a widespread view that good data ethics is a 'good thing' but what does this mean in practice and how can it be maintained as technology changes? Arbitrary decisions about what is 'ethical' in data use that are taken on the spur of the moment, perhaps when a problem or opportunity arises, is likely to lead to bias if not abuse. Better to have a set of 'data ethics principles' established that all can see and abide by, making the 'red lines' clear in advance.

Politicians have a clear role here is setting and observing standards of data ethics, shaping the ethical culture and tone of the organisation. When this does not happen, it is clear that others take it for granted that data ethics does not matter (you can find your own examples of this).

It is also becoming more compelling as AI (artificial intelligence) , ML (machine learning) and RPA (robotic process automation) take off, hiding much of the complex decision making in machine level judgements and data linkages. If the principles are not clear in how they are code and used, and if there are no safety check in place to detect deliberate or unintended abuse, problems will undoubtedly arise. For example, can an AI system always judge what is best for an individual without human intervention?

But it also needs public support. If citizens are complacent or indifferent, it is harder for public bodies to justify the time and investment necessary to ensure high levels of integrity in data use.

A simple definition of data ethics:

"no adverse impact and no unintended or deliberate bias"

"Privileged access to data undermines public trust. It creates opportunities for figures to be 'spun' to the media or 'buried'".

On Lies and Statistics – The Royal Statistical Society, Nov 2017

Principles of data ethics

1. Honesty and trust are prioritised, at all times and especially in personal data. This means that there is clear accountability and responsibility for ensuring data ethic principles exist and are adhered to

2. Openness and transparency, trump 'closed and confidential', without compromising security and privacy or requests for anonymity. This means sharing and being clear about why and how data is captured and used

3. Safety in use – confidence in data quality, and in data for decision-making. This includes user consent in how personal data is used and ensuring public and personal good is prioritised over commercial interests or business efficiency

4. Data is owned by people, not departments or even organisations (they are custodians). This means that the organisation genuinely 'listens' to its data, to avoid unintended (or deliberate) prejudices – it uses automated and manual practices to achieve this openly

5. Data custodians ensure that the purpose of data collection, its processing and storage are in the public's interest. This means that data is not used for political, business or private benefit unless this was made clear when collected

6. Security and cyber procedures are there to protect data and public interest. This means that As AI systems develop, there are checks to maintain 'public good' principles, avoidance of bias, and manual intervention to correct and prevent errors

7. Data provenance is always validated and never just assumed, especially in complex or significant decision-making scenarios. This includes adopting data cleansing procedures with a commitment to and strive for high data quality

1. Necessary training, advice and support is given to data users, citizens, business leaders, politicians, suppliers and partners receive necessary advice, support and training to ensure the whole systems of data management follows strong ethical principles

2. Open APIs and opensource are used wherever possible, with common industry standard data formats and no data lock-in from IT systems providers permitted. Commercial reuse of public data or personal data does not happen without agreement

3. Data processing practices are designed to ensure equality, reflecting the different groups in society , especially vulnerable people, to avoid discrimination, disenfranchisement or stigma.

4. Accountability and responsibility is clear in governance and practices, so that breaches can be quickly detected and learnt from, rather than hidden. This includes working closely with partners outside the organisation to encourage good practice.

5. Human intervention exists as a safety valve, especially in AI systems and automated decision-making systems. IT tracking apps are used to identify risks and to alert to changes in inappropriate use. They are not used to track individuals without their consent

These are just examples and there are many more on the internet to choose from!

Contract for the web - Sir Tim Berners-Lee

"The Web was designed to bring people together and make knowledge freely available. It has changed the world for good and improved the lives of billions. Yet, many people are still unable to access its benefits and, for others, the Web comes with too many unacceptable costs. Everyone has a role to play in safeguarding the future of the Web. The Contract for the Web was created by representatives from over 80 organisations, representing governments, companies and civil society, and sets out commitments to guide digital policy agendas. To achieve the Contract's goals, governments, companies, civil society and individuals must commit to sustained policy development, advocacy, and implementation of the Contract text."

Sir Tim Berners-Lee, 2019

Much of the recent work by Sir Tim Berners Lee is about information and data on the Web. Originally this was about open and linked data, to help make information as freely and readily available to as many people as possible. Today his concerns are as much about wrongful information exploitational and use – both deliberate and unintentional. It is about the dominance of a few global institutions and how they use our data. And it is about governments introducing the necessary regulation, control and ethical practice to protect us all and to ensure information is used for public good.

Launched in 2019, his 'Contract for the Web' provides a strong foundation for internet and data use, and should be read and embraced by all public service organisations.

Equality, privacy and trust

Protecting people's privacy, ensuring thrust is earned and maintained, and equality achieved in service provision as delivery becomes increasingly digitised requires a sophisticated response, underpinned by a clear code of ethics. But it is also more than ensuring good intentions and well-designed principles. There are also a range of practical steps that need to be taken:

- How do we know that we have achieved digital inclusion and equality in how digital solutions are implemented?
- How are the risks of bias and prejudice in digital systems, and especially AI technologies, being managed and detected?
- Have we trained staff in these risks and the policy ambitions we have set?

Equality, privacy and trust

Equality and Discrimination

Particular care needs to be take in AI systems, where machine learning is already being deployed in the public sector to support decision making – which prisoners to release? What package of care is best? Which candidates should we appoint? Where should we build? Redirect traffic: the list goes on. There is a challenge in protecting the interests of vulnerable people or minority groups who often do not get represented well-enough, because of inherent bias towards 'the average' in learning systems. And and even when such systems are designed to remove human bias, they can unintentionally reinforce it, unless there is careful design, transparency and human oversight. Checks should be introduced to detect and correct such bias, deliberate or accidental.

Privacy

Privacy is always a concern in any government system, and the public rate it very highly in the UK (seen in the concern in the past over ID cards). Yet there are still privacy risks when perhaps there is a view that the 'greater good' outweighs individual rights, seen in some inadvertent government projects to share personal data with Google and others in order to secure better health insight and learning, but with at least a perceived risk of privacy being compromised in certain cases. It is also not as simple as saying privacy always comes first, because there will be cases where there is an indisputable need to disclose personal data – for example a child at risk or if someone suspected of potentially malicious intentions. So systems and policies need to be clear on the exceptions to privacy and how these will operate with due control, transparency and authority.

Trust

Trust comes from practice. A reputation can only ever learn trust by its practice and habits – and equally it can be lost overnight. It is not about avoiding every possible error, but more about openness and in how incidents are dealt with. A GDPR breach, if well-managed, can increase trust over time, provided the organisation demonstrates that it has learned, that it has clear and strong intentions in the right place, that its leaders are accountable and that mistakes are neither repeated nor covered up.

Additional resources

- ODI resources:
  - The Data Ethics Canvas (as part of the Data and Public Services Toolkit)
  - Introduction to data ethics and the Data Ethics Canvas training
  - Monitoring equality in digital public services report
  - About data about us: data rights and ownership project
- The ethical impact of data science https://royalsocietypublishing.org/toc/rsta/374/2083
- Data4Good news (UKAuthority) https://www.ukauthority.com/topics/data4good/
- Data Ethics principles (Daaethics) https://dataethics.eu/data-ethics-principles/
- Data Ethics framework (Gov.uk) https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework
- Universal data principles (Accenture) https://www.accenture.com/_acnmedia/pdf-24/accenture-universal-principles-data-ethics.pdf

Case studies

- Predicting gang exploitation (The Guardian) https://www.theguardian.com/society/2018/sep/17/data-on-thousands-of-children-used-to-predict-risk-of-gang-exploitation
- Predicting child abuse (The Guardian) https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse