Helping organisations navigate ethical concerns in their data practices

September 2017

Open Data Institute

Table of contents

Authors: Ellen Broad, Amanda Smith and Peter Wells
Editors: Anna Scott and Charlotte Fleming
Design: Adrian Philpott and Christie Brewster

Executive summary

Data ethics is a rapidly emerging area. Increasingly, those collecting, sharing and working with data are exploring the ethics of their practices and, in some cases, being forced to confront those ethics in the face of public criticism.

Codes of data ethics are being developed across sectors, ethics training is becoming more common and debates are accelerating on issues like the monetisation of personal data, bias in data sources and algorithms, and the consequences of under-representation in data.

Building trust

For some time, the Open Data Institute has been working on measures to help organisations build trust in how they collect, use and share data, and to foster better use of data overall.[1] Trust is an essential component of society. When trust breaks down, the public lose faith in the institutions that provide them with services, and organisations lose the ability to share data and collaborate in ways that could improve all our lives.

This paper starts by exploring the relationship between data ethics and legal compliance, some existing data ethics frameworks and ethical considerations in data collection, sharing and use.

After this exploration – and considering the challenge of agreeing practical data ethics frameworks for sectors, societies or globally that it highlights – we offer an approach, the Data Ethics Canvas, for organisations to identify and manage data ethics considerations.

Challenging common assumptions

By exploring data ethics in depth, we uncovered common assumptions about data ethics that we wanted to challenge.

[1] See: https://theodi.org/open-data-in-government-how-to-bring-about-change; https://theodi.org/blog/policy-design-patterns-that-help-you-use-data-to-create-impact; https://theodi.org/guides/openness-principles-for-organisations-handling-personal-data

1. ‘**Data ethics is only an issue where activities involve personal data.**’ Ethics issues must also be considered in the collection and use of non-personal data. For example, not publishing the location of bus stops in poorer neighbourhoods can mean that the advantages of smartphone-mapping and route-finding services are not available to people who live in those areas, increasing existing inequalities.
2. ‘**Data ethics is concerned with data protection compliance.**’ Complying with legal obligations – under the EU General Data Protection Regulation, for example – is just one part of treating data ethically. Data-related activity can be unethical but still lawful.
3. ‘**Data ethics is (only) about how organisations use data.**’ Data ethics is about the impact that all data activities have on people and society. Collecting and sharing data only about certain groups of people may disadvantage them relative to others. All activities should be subject to ethical examination.

We intend to raise awareness of the kinds of ethics issues – involving both personal and non-personal data – that can arise from how data is collected, who it is shared with and what it is used for. The paper uses case studies to explore the ethical issues that may arise either through malicious or non-malicious intent but due to a lack of proper consideration before data is collected, shared and used.

To help increase the level of consideration we developed the **Data Ethics Canvas**, a prototype – for identifying potential data ethics issues associated with a data project or activity. It is based on the Ethics Canvas,[2] a tool for assessing the ethical implications of any project designed by the ADAPT Centre for Digital Content Technology (CC-BY-SA), which is itself based on the original Business Model Canvas by Alex Osterwalder.[3]

We hope to see the Data Ethics Canvas used by teams starting new data activities. It is designed to be collaborative, involving people from across teams with different perspectives.

We will continue to test and improve the Data Ethics Canvas in the months to come, and would welcome feedback and ideas. The Data Ethics Canvas and a user guide are included in the appendix of this report. **You can write to us at policy@theodi.org.**

This report has been delivered through a collaborative partnership between ODI and Arup, the global consultancy firm. Arup has worked with ODI since 2014 to showcase and develop the use of open data.

[2] https://www.ethicscanvas.org.
[3] https://strategyzer.com/canvas/business-model-canvas.

Introduction

Ethics help us to navigate what is right and wrong in the work we do, the decisions we make and the expectations we have of the institutions that impact on our lives. Across sectors – from medicine, bioscience and journalism to government, research and statistics – codes of ethics have been created and updated as people confront the moral problems of their time.

The last decade has seen the rise of an age of data abundance. New technologies and mechanisms for harnessing data increasingly affect our day-to-day lives – from machine-learning to robotics, automated services to smart devices – making it possible for people with disabilities to live more fulfilling lives or people with smartphones to more easily navigate their cities.

The increased amount of and use of data calls into questions pressing issues of fairness, responsibility and accountability, and whether existing legislation is fit to safeguard against harm to an individual or group's privacy, welfare or physical safety.

Data ethics is a branch of ethics that is addressing these questions and shaping the context in which organisations collecting, using and sharing data operate. Increasingly, sectors and organisations are being called upon to develop their own data ethics principles, policies and processes. A number of existing data ethics frameworks and principles are explored in this paper. This exploration should help people to understand the current landscape and why we chose to develop the Data Ethics Canvas.

What is data ethics?

In a paper for the Royal Society in late 2016, researchers Luciano Floridi and Mariarosaria Toddeo define data ethics as:

"The branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (e.g. right conducts or right values)."[4]

At the ODI, we believe short and accessible definitions are necessary to include more people in debates that impact them. We suggest and use a different data ethics definition of: **a branch of ethics that evaluates data practices with the potential to adversely impact on people and society – in data collection, sharing and use.**

[4] http://rsta.royalsocietypublishing.org/content/374/2083/20160360#sec-1.

The relationship between data ethics and legal compliance

Compliance with relevant legislation and regulation is part of handling data ethically and data ethics templates must take compliance into account. It is possible that breaking the law can be done in the interests of ethics. However, in cases where ethics and societal norms contradict legal compliance it is likely that the law needs updating. Existing legislation has often been developed due to prior ethical debates.

This section provides a high-level overview of the current legal context shaping access, use and sharing of data that forms part of the backdrop for any data ethics framework. It is focused on UK and European Union legal frameworks. It includes both legislation that is explicitly related to data, such as data protection, and legislation that has a wider scope, such as anti-discrimination and consumer protection.

Understanding the breadth and history of such legislation helps people working with data ethics to understand the environment and prior work that they are building on.

The recent history of privacy laws

While data ethics has only been established as a discrete branch of ethics in the last half-decade, changing attitudes to data – often in response to new technologies and innovations – have been influencing legal reform for nearly half a century. The evolution of data protection laws reflects changing expectations of privacy and consumer control. Data security and storage laws impose responsibilities on organisations storing sensitive data. Intellectual property (IP) and database laws reflect expectations of being able to extract value from investing in collecting and organising data.

In 1980, the Office for Economic Cooperation & Development (OECD) published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[5] The opening sentence of the preface remains relevant today:

> *"The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data."*

[5] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

The OECD guidelines attempted to combine the existing privacy laws and build consensus around basic principles that would underpin future legislative intervention. The guidelines informed the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data, a 1981 Council of Europe Treaty which recognised a right to privacy within the context of increased personal data flows across national borders.[6] The OECD principles were reflected in the UK's first Data Protection Act in 1984, and some of the OECD principles are still reflected in the UK and European Union's data protection laws today.[7]

A right to privacy also exists under human rights law. It is recognised in Article 8 of the European Convention on Human Rights (and reflected in the UK Human Rights Act 1998),[8] entitled a 'right to respect for family and private life'. 'Private life' refers to things like a person's sexuality, body, personal identity, family and relationships, and their personal information. It is an open-ended provision that also allows a number of exceptions for national security, public safety, the economic wellbeing of a country, protection of health and protection of the freedoms of others. The EU Charter of Fundamental Rights also recognises a right to the protection of personal data (Article 8).[9]

Data protection laws in Europe today

In 1995, the European Union adopted the Data Protection Directive, intended to unify data protection legislation across EU member states.[10] The Data Protection Directive will be superseded by the General Data Protection Regulation (GDPR) when it comes into force on 25 May 2018. The GDPR is designed to give European citizens greater control over personal data against a backdrop of increasing automation, expanding mobile connectivity, government and corporate surveillance, and large-scale commercial hacks of sensitive personal data.[11]

The GDPR updates the rights of people (or 'data subjects') in how data about them is collected, stored, managed and used, and expands existing ones. It updates the right of data erasure (a 'right to be forgotten') and rights to data amendment. It introduces a new right of data portability which allows individuals to obtain and reuse personal data about themselves and

[6] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[7] Schedule 1, Data Protection Act 1998 (UK). Interestingly, while openness about development of data processes and policies is a principle of the OECD guidelines, it is not reflected in the UK's Data Protection Act.

[8] http://www.legislation.gov.uk/ukpga/1998/42/schedule/1.

[9] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:html.

[11] See for example the Sony Pictures hack (2014) of employee emails, salaries, unreleased films and other employee personal data; Home Depot (2014) and Target (2013) breaches of customer credit card data; Ashley Madison leak of customer records (2015).

share it for their own purposes across different services (ICO, 2017).[12] The GDPR expands the responsibilities (and liabilities) for organisations managing or processing personal data. Under Article 35 of the GDPR, mandatory Data Protection Impact Assessments (DPIAs)[13] are introduced where the processing is likely to result in a high risk to the rights and freedoms of individuals (in particular when using new technologies).[14] Several aspects of the GDPR inform this paper.

While the UK has commenced negotiations to leave the European Union, the UK Government has confirmed its intention to implement the GDPR and bring in a new Data Protection Bill that is understood to include the provisions of the GDPR.[15] The ODI has developed both principles and guidance for organisations collecting and processing personal data that incorporates obligations under the GDPR.[16]

Intellectual property and database laws

Intellectual property laws can influence how organisations and individuals collect, process and share data. In the EU, as well as potential copyright rights in data, the database right awards a property right for substantial investment by people and organisations in obtaining, verifying or presenting the contents of a database.[17] This restricts how organisations might access, copy, monetise, amend or share data belonging to someone else.

In circumstances where a database right exists, for example, an organisation collecting, scraping (extracting data from websites) or otherwise accessing data from a third party, the organisation needs to be sure that what they are doing is lawful: that they have sought permission from the data owner, or accessed the data under an open licence or other licence that permits what they are trying to do.

[12] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability.

[13] Privacy Impact Assessments (PIAs), which were already promoted by the UK Information Commissioner's Office as best practice.

[14] Note: not all new technologies involve a likely high risk to individuals.

[15] https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law.

[16] https://theodi.org/guides/openness-principles-for-organisations-handling-personal-data.

[17] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Article 7.

Laws relating to confidential information

On 8 June 2016 the European Parliament and Council adopted the Trade Secrets Directive, standardising corresponding national laws in member states.[18] It covers both long-held, strategic information held by a company (e.g. a secret recipe or a chemical compound) and short-lived information, such as the results of a marketing study or the launch date of a new product.[19] It is strictly concerned with circumstances in which confidential information has been misappropriated.

Laws relating to the treatment of trade secrets and confidential information of this nature exist in many national jurisdictions. While it is typically rare that organisations handling data will find themselves in breach of laws relating to trade secrets – unless they unlawfully acquired that information – they are included here as part of the regulatory context shaping data ethics debates.

Laws relating to anti-discrimination

Societal attitudes towards discrimination and expectations of accountability, fairness and equal treatment have also evolved over time, and are reflected in varying legislation across sectors.

Employers are expected to provide a basic duty of care to employees and safe workplaces under occupational health and safety laws. Consumers are protected from unfair treatment by goods and service providers under consumer protection laws. Organisations and individuals must take care to avoid causing harm to people or property or risk being accused of negligence, while fairness and equal treatment are reflected in anti-discrimination laws pertaining to age, race, sexuality, gender, religion and disabilities.

The Universal Declaration of Human Rights (UDHR) – proclaimed by the UN General Assembly in 1948 – recognises that every person is entitled to economic rights, social rights including education, and rights to cultural and political participation and civil liberty. Article 2 of the UDHR asserts that these rights apply equally to every person:

> *"[...] without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."*[20]

[18] http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en.
[19] Ibid.
[20] Article 2, Universal Declaration of Human Rights (1948): http://www.un.org/en/universal-declaration-human-rights/index.

The International Covenants on Economic, Social and Cultural Rights and Civil and Political Rights (1966) affirm and expand on these rights. These covenants and other international human rights instruments have shaped regional and domestic laws regarding anti-discrimination,[21] including the UK's Equality Act 2010.[22]

Laws relating to anti-discrimination reflect societal expectations of fair and equal treatment. They inform ethical considerations regarding data collection, sharing and use – that data practices be free of bias and inaccuracies that may lead to discrimination against people or groups of people, and that in practice people are not discriminated against. While they are not specific to data, they should not be forgotten by data ethics.

[21] See for example the Convention on the Rights of the Child (1989) and the Convention on the Elimination of all forms of Racial Discrimination (1965).

[22] http://www.legislation.gov.uk/ukpga/2010/15/contents.

Existing data ethics frameworks

To inform the Data Ethics Canvas we considered existing data ethics frameworks and principles from government, research and industry sectors. There is much work being undertaken in this space and it will continue to evolve. This paper is not intended to look at the landscape comprehensively, and we are capturing data ethics frameworks as we discover them.

Existing data ethics frameworks explored included:

- The UK Government Data Science Ethics Framework (launched May 2016)[23]
- Ethical guidelines for data protection and privacy, drafted by the European Commission's FP7 working group (2009)[24]
- UK National Statistician's Data Ethics Advisory Committee principles[25]
- The Jisc code of practice for educational institutions undertaking learning analytics (2015)[26]
- The US Farm Bureau's privacy and security guidelines for farmer data (2016)[27]

Across those explored, common elements included:

- that any **collection and use of data is fair and lawful**
- that any personal data collected from people is **collected for a specific purpose**, and only used for that purpose (or for future uses that are not 'incompatible' with that original purpose)
- that any **collection of personal data not be excessive**; simply what is required for meeting that original purpose
- that organisations managing personal data be **open about their processes, policies, uses and collection of personal data**

To a lesser extent (depending on context), some of the data ethics frameworks included:

- **a requirement that any collection and use of data be based on a clear user need**, and/or with public benefit (this is part of the UK Government Data Science Ethics framework)
- **formal recognition that people supplying personal data own the data that is about them** and their livelihood, families and property.[28] This is becoming an

[23] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524298/Data_science_ethics_framework_v1.0_for_publication__1_.pdf.

[24] http://ec.europa.eu/research/participants/data/ref/fp7/89827/privacy_en.pdf.

[25] https://www.statisticsauthority.gov.uk/national-statistician/national-statisticians-data-ethics-advisory-committee.

[26] https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics.

[27] http://www.fb.org/tmp/uploads/PrivacyAndSecurityPrinciplesForFarmData.pdf.

[28] Complexities surrounding 'ownership' language with respect to personal data have been documented by the ODI in '*How do we own data?*': https://theodi.org/blog/how-do-we-own-data. 'Ownership' is the language used by the US Farm Bureau in their principles.

increasing concern in agriculture, where data about weather, soil conditions, pesticides used, crop yield and growth are collected from farmers, without clear ownership rights in place.

- **Recognition that a person's choice to provide personal data may not be a wholly free choice.** The Farm Bureau guidelines require organisations collecting personal data to explain the effects and abilities of a farmer's decision to opt in, opt out or disable the availability of services and features offered by the ATP. If multiple options are offered, farmers should be able to choose some, all, or none of the options offered.

Many of these elements place conditions around how data is stored, processed and shared (and who has access), as a way to guard against unethical use. However, they do not enable critical thinking about the ways in which people might be affected by a project, which validates whether the conditions placed on data use are proportionate.

The frameworks explored are, on the whole, concerned with the ethical treatment of **personal data**. The ethics framework that most applies to broader data use is the UK National Statistician's Data Ethics Advisory Committee principles.[29] Across most frameworks studied, safeguarding privacy, empowering data subjects with control over how personal data is used, and protecting against data breaches were key themes. These are essential considerations for any project involving use of personal data.

However, in our research we saw gaps in existing frameworks. We see the need to expand conceptions of data ethics in future ethics codes and frameworks to include:

- circumstances **not involving personal data**
- at **any stage of a data handling activity:**
  - data collection
  - data sharing
  - data use (including the design of models and algorithms)
- issues **outside of privacy and user control**, such as:
  - bias in data and data model design
  - anti-competitive practices
  - practices that reinforce inequalities or stereotypes
  - practices that propagate falsehoods
  - inaccuracies in data
  - margin for error

[29] https://www.statisticsauthority.gov.uk/national-statistician/national-statisticians-data-ethics-advisory-committee.

Organisations navigating data ethics require tools that help them survey the **impact of their data use or project**, to help understand how choices made might be considered ‘right’ or ‘wrong’. The Data Ethics Canvas proposes a new approach, with **impact on people and society at its core**.

A data project can involve only non-personal data and still be unethical

Issues of bias, inaccuracies and inconsistencies in data can arise regardless of the nature of its source, whether personal or non-personal. Researchers analysing trends in aggregated search-engine data, for example, must account for gaps in who has contributed to that data (a predominantly digitally literate population). Identifying and mitigating issues within data sources that could negatively affect certain population demographics if left untreated is part of treating data ethically.

Case study: It is more expensive to play Pokemon Go in minority neighbourhoods

Pokemon (short for the original Japanese title of ‘Pocket Monsters’) is a popular franchise owned by Nintendo with two other companies (Game Freak and Creatures). Pokemon are imaginary creatures and players (known as trainers) can catch these animals and use them to battle other trainers.

Pokemon Go is a free-to-play, location-based augmented reality game developed by Niantic in collaboration with Nintendo. In the game, players use their mobile device GPS to locate, capture, battle and train virtual Pokemon. Players collect ‘pokeballs’ – needed to catch pokemon, and therefore to play the game – from pokestops (check points) and battle other pokemon at ‘gyms’, which are based on their GPS location. Without access to pokestops, players must pay for pokeballs and other items. Players with easy access to pokestops and gyms, on the other hand, can earn more experience points and collect more items for free.

The locations of pokestops and gyms in Pokemon Go were derived by Niantic from the locations of ‘portals’ in a previous augmented-reality GPS-based game, Ingress.

Locations for Ingress were predominantly crowd-sourced, both via an existing database – Historical Marker Database – and by Ingress players. The Historical Marker Database reflected contributions from approximately 3,000 volunteers across the US who were mostly male. Ingress players also appeared to be mainly male, young and English-speaking. [30]

When Pokemon Go was released, users noted that pokestops and gyms occurred much less frequently in poor neighbourhoods, and black and other minority neighbourhoods.[31] In New York City, for example, pokestops were densely populated in Manhattan but sparse in outer boroughs, particularly Brooklyn and Queens, where higher percentages of the population are from minorities. Portals were densest in majority white and asian neighbourhoods.[32]

Studying the locations of Pokestops, derived from Ingress data, exposes the limitations of crowd-sourced data. In Pokemon Go – which has had significantly broader reach than Ingress – gaps in the underlying pokestop location data stand to potentially drive up the cost of playing Pokemon Go for users in predominantly black, hispanic or low socio-economic neighbourhoods.

The underlying data sources for the locations of pokestops in Pokemon Go are non-personal, however these geolocation gaps stand to negatively impact on certain Pokemon Go users (by increasing the overall cost of participation). A data ethics framework that helps people to identify how data use affects different demographics could have helped identify this issue before the launch of the game and allowed the developer to take steps to mitigate the issue and broaden the pool of players.

[30] http://www.miamiherald.com/news/nation-world/national/article89562297.html.
[31] Ibid.
[32] Ibid.

Data collection

Ethical issues that arise from data collection if not identified and mitigated may result in harm to individuals or a community. If you are collecting or creating a dataset for the first time – or using existing data sources – consider whether any gaps, inaccuracies or bias might exist in your information sources.

Gaps in data

Data omissions do not always cause direct harm, but where a limited data source is used to generate insights about a larger population or provide a service at scale, omissions can have negative impacts. The Pokemon Go case study offers an example of how gaps in data sources – despite having limited impact on their original users – can negatively impact on members of a community when used for a wider service.

The absence of certain fields or categories of information in a data source can reflect a historic bias. In the UK, for example, the 'prescribed particulars' of a marriage still only require the father's name and occupation, not the mother's.[33] The omission of information about a mother's name and occupation has follow-on effects in fields like genealogy, sociology and history. It is easier for people to analyse how male occupations evolved over the centuries than it is for those of females.

Where data is crowdsourced, gaps in the representation of certain population demographics need to be taken into account. Social media feeds like Twitter and Facebook are being mined and analysed for everything from forecasting influenza outbreaks[34] to responding to natural disasters.[35]

Their limitations as data sources from which to gain insights about a wide population are well known. For example, in the US, a 2016 survey from the Pew Research Centre of adults using social media indicated that approximately 79% of US-based adults were on Facebook; 24% on Twitter; 32% on Instagram; and 29% on LinkedIn.[36] Also, user demographics of each of these services varied: women were more likely to use Facebook than men; Instagram users tended to be younger, with more women online likely to use Instagram than men; Twitter was more popular among highly educated users.[37]

[33] http://theodi.org/blog/pressure-still-needed-to-put-mothers-names-on-marriage-certificates.
[34] http://currents.plos.org/outbreaks/article/twitter-improves-influenza-forecasting.
[35] http://www.iflscience.com/technology/twitter-tracks-intensity-natural-disasters.
[36] http://www.pewinternet.org/2016/11/11/social-media-update-2016.
[37] Ibid.

Finally, not all adults use social media or go online. In the UK, the Office for National Statistics found in 2016 that 10.2% of the population had never used the Internet.[38]

Typically, data scientists and social researchers take the limitations of social media datasets into account in their research design and the insights they present. But relying simply on social media data – without accounting for gaps in the data source – would skew an emergency response towards digitally literate, mobile, active internet users and risk negatively affecting vulnerable members of a population – the elderly, poor or recent migrants, for example.

Bias in data

There are several ways in which bias in data can arise. Bias can result from:

- survey questions being constructed by people with a particular intent or framing
- selectively collecting data from groups with particular backgrounds
- underlying bias in people from whom data is sourced

The following two case studies show some of the ways in which biases can occur.

Case study: Trialling facial recognition software to identify potential offenders

A 2016 machine-learning paper from Shanghai Jiao Tong University investigated whether criminality in humans could be detected based on analysis of facial features.[39] They collected 1856 ID photos of Chinese males aged between 18 and 55, controlling for certain features (no facial hair, scars etc), which was divided into subsets of 'non-criminals' and 'criminals', respectively. The images of non-criminals were gleaned from the internet. ID photos – not mugshots – of criminals were provided by police departments and the ministry of public security.

Using machine-learning techniques, the researchers identified certain discriminating structural features for predicting criminality, such as lip curvature, eye inner corner distance and a 'nose-mouth angle'. They concluded that the faces of general law-abiding

[38] https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2016.
[39] https://arxiv.org/pdf/1611.04135v1.pdf.

citizens had a greater degree of resemblance compared with the faces of criminals and that criminals' facial features were more varied.

Since its release, the paper has been criticised for failing to account for underlying bias in how the photos of offenders had been collected, and for an overreliance on machine-learning techniques to infer criminality, at the expense of insights from criminology and physiology.[40]

The paper does not reflect on whether the ID photos of criminals reflect wider bias in terms of who in Chinese society is more likely to be arrested (increasing the chances, among this portion of the population, that someone will be found to have committed a crime). If a member of the population 'looks different', they are more likely to be suspected of committing a crime. With those accused of committing crimes more likely to be members of a population who 'look different' from the general population, conviction is going to reflect this skewed focus on that segment of the population.

[40] https://motherboard.vice.com/en_us/article/new-program-decides-criminality-from-facial-features.

Case study: Developing sentencing algorithms to predict the likelihood of reoffending

In the US, sentencing algorithms, called 'risk assessments', have been developed to predict the likelihood of further criminal behaviour and adjust offender supervision appropriately.[41] Propublica – a US-based non-profit media organisation – obtained the risk scores assigned to more than 7,000 people arrested in Broward County, Florida in 2013–2014, based on one such algorithm, and measured them against actual rates of reoffending. Propublica observed that of those deemed likely to reoffend, 61% were arrested for subsequent crimes within two years.[42] They found that the formula was particularly likely to falsely predict black defendants as future criminals at twice the rate of white defendants. White defendants were more likely to be mislabelled as low-risk but go on to reoffend than black defendants.

[41] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[42] Ibid.

The sentencing algorithm analysed by Propublica was designed by a for-profit company, Northpointe. Their core product is a set of risk scores derived from 137 questions in a survey, answered by defendants or extracted from criminal records. While ethnicity is not an explicit question in the survey, several questions posed are likely to increase the risk scores among black defendants. Questions asked include: 'Has one of your parents ever been sent to jail or prison?' and 'How many of your friends/acquaintances are taking drugs illegally?' In the US, black children are more than seven times more likely than white children to have a parent in prison.[43] The 2014 US National Survey on Drug Use and Health indicated that as of 2014, the rate of illegal drug use among African Americans (ages 12 and over) per month was 12.4%, above a national average of 10.2%.[44] The higher likelihood that a black defendant had a family member who was incarcerated and/or an acquaintance using drugs illegally influenced their risk scores adversely.

[43] https://www.prisonfellowship.org/resources/training-resources/family/ministry-basics/faqs-about-children-of-prisoners.

[44] https://www.samhsa.gov/specific-populations/racial-ethnic-minority.

It can be difficult for a single organisation or researcher to spot and eliminate bias. Some startups and organisations are beginning to open up their data sources and the algorithms they have created to enable feedback on whether any bias or other gaps or inaccuracies exist. A predictive policing startup in the US, CivicScape, released its algorithms and data, along with documentation detailing how its algorithm worked via Github to enable greater scrutiny.

> *"By making our code and data open-source, we are inviting feedback and conversation about CivicScape in the belief that many eyes make our tools better for all […] We must understand and measure bias in crime data that can result in disparate public safety outcomes within a community."*[45]

Data ethics frameworks should encourage openness about how data is proposed to be used and include a section on '*how can people engage with you?*' to help organisations to consider and describe choices made in the design of their data models and systems, what measures are in place to address errors and enable feedback, and whether the appeal mechanisms put in place are reasonable. As a result of considering these decisions, organisations might decide to change them.

[45] https://github.com/CivicScape/CivicScape/blob/master/evaluation_notebooks/notebooks/PreventingBias.ipynb.

Unlawful data collection

The circumstances in which data has been collected can give rise to questions of ethics and questions of legality. Data might be acquired unlawfully – in breach of intellectual property laws, laws relating to confidential information, or data protection laws. Where data projects involve pre-existing data sources, it can be difficult, if not impossible, to determine whether these sources were collected from lawfully – because there might be no documentation regarding the origin of data sources, and because laws surrounding data collection can be complex.

Having access to an organisation's commercially sensitive product data, for example, without any evidence of permission or involvement from that organisation, may indicate that it has been acquired unlawfully by someone, and influence decisions made about how that data should be used.

Some data collection might not be unlawful but can still be unethical. Instances of data collection relating to indigenous populations offer an example of this. In South Africa, the San people have issued a code of ethics for researchers which requires (among other things) that consent be granted before photos are taken or published of San individuals, and that approval for research proposals be granted by the San councils before research is undertaken.[46]

Data sharing

Data exists on a spectrum, ranging from closed to shared to open.

Shared data is data provided to restricted organisations or individuals. Sharing data is essential to maximising its benefits, and can be done in a variety of ways.

- Data can be **shared with a specific individual or group** of individuals (for example, a doctor might share a patient's x-rays with a surgeon and hospital team).
- Data might be **made available to certain accredited** or **authorised entities** via a secure data-sharing platform.
- Social media data might be purchased by researchers and companies hoping to understand consumer trends.

An organisation can also make their data available as open data: **data that anyone can access, use and share.**

[46] http://www.smithsonianmag.com/smart-news/san-people-south-africa-issue-code-ethics-researchers-180962615.

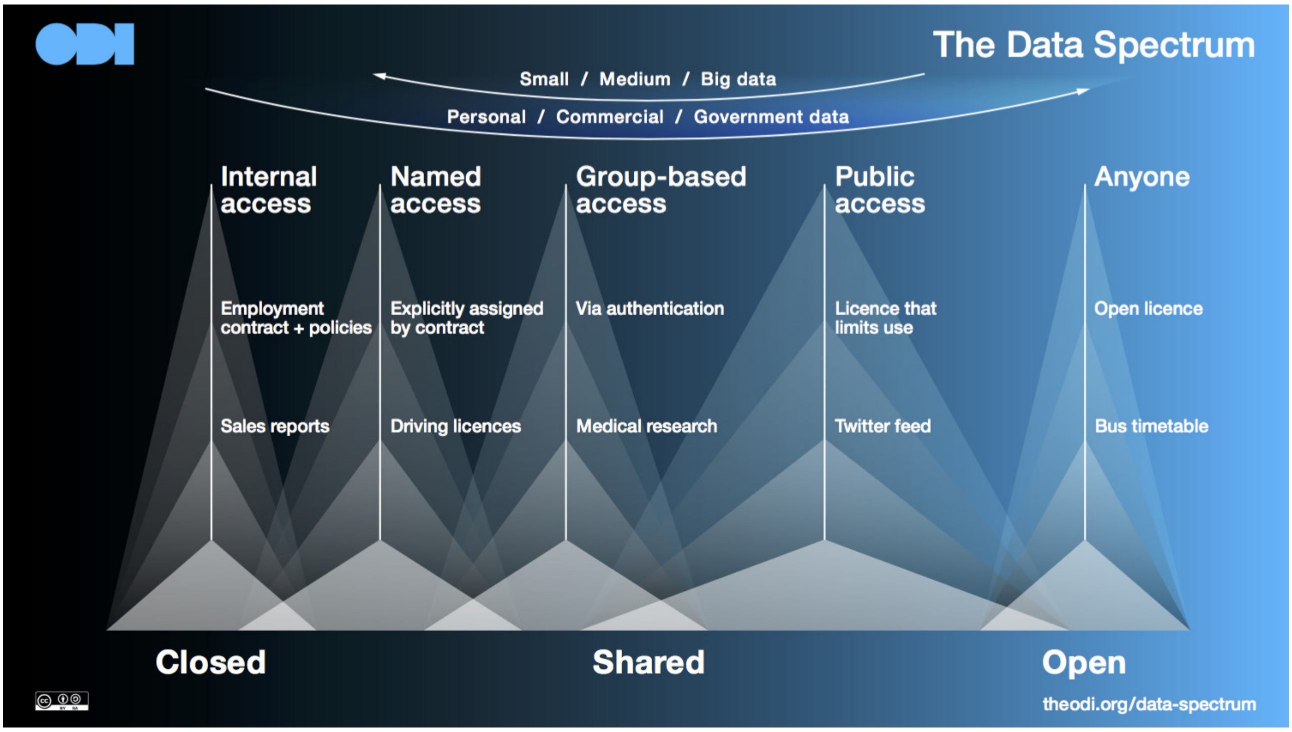

Figure 1: The Data Spectrum

How we share data is shaped by the nature of the data in question, the circumstances in which it has been collected and laws that restrict its distribution. Sometimes terms and conditions attached to data collection – surveys, questionnaires, signups for services – guarantee that individual survey responses will not be shared. When accessing medical services, we often agree to our health data being shared in specific ways. Limits to how data is shared and with whom can be explicit or implicit. Data protection laws, intellectual property laws and laws relating to confidential information also shape who will have access to data.

Sharing data knowing that it may cause harm to individuals or society

Agreeing to provide data to organisations or individuals where you are aware it could reasonably result in harm creates ethics concerns. 'Harm' can be direct or indirect. Harm could result from disadvantage or prejudice arising from how the data is used by the organisation with whom it is shared; it could be physical harm, if exposure of certain kinds of information poses threats to people's safety. This can occur even where the distribution of that data is lawful. Publishing the details of abortion providers – names, clinic locations and hours – in a country or region where you know they are likely to be the target of violence may be unethical, even if the publication of that information is lawful. How and where the information is published is important, people who need an abortion need to be able to find a provider but abortion providers need to be protected from malicious actions.

The US government recently passed a law repealing changes to online privacy rules for US citizens introduced by the previous administration. This included requirements that Internet Service Providers (ISPs) – organisations that provide access to the internet – obtain consumers' consent before sharing or selling their browsing information and other data.[47]

While ISPs in the US can now lawfully record and sell a citizen's browsing history, to whom it is sold can pose ethical issues – for example, to predatory loan companies, known scam operations or organisations that may use a citizen's browsing history to target, blackmail or unfairly affect them. Being mindful of who has access to data you have collected, what risk of harm or prejudice might arise from that access, and taking steps to mitigate that, is part of taking responsibility for the impact that data you share may have on people and society. In some circumstances, organisations may make a decision not to collect certain kinds of data, so as to avoid potential misuse by others.

Creating unfair monopolies

Unfair monopolies can arise where data access is restricted to one organisation or a small number of organisations, where it might otherwise reasonably be shared. Again, whether an exclusive arrangement can be said to be unethical will depend on circumstances. In the European Union, exclusive arrangements regarding access to public sector data are prohibited – with some limited exceptions – by the Directive on the Re-use of Public Sector Information (PSI).[48]

Exclusive arrangements are prohibited under the PSI regulations because they prevent others from benefiting from public sector data and can restrict competition. The potential uses of a data asset – medical research, disease prevention or natural disaster planning, for example – may require it to be accessible to more than one organisation.

[47] SJ Res 34: "A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services". March 28 2017: https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34 . Note: the original law was due to come into effect in 2017, and now no changes will take place.

[48] Article 11, Directive 2003/98/EC Directive on the Reuse of Public Sector Information https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information.

Increasingly, private sector data providers also provide infrastructure for organisations and individuals analysing data, with lock-in effects. In agriculture, organisations like Climate Corp (headquartered in San Francisco) are transitioning from providing farmers with insights based on existing open and proprietary data sources, to providing physical sensor infrastructure in fields monitoring things like soil quality, moisture and temperature.[49]

Ethical issues may arise where the terms of service associated with physical data infrastructure and the data they collect – via smart meters, field sensors and smart cars – prevent people in practice from switching providers and accessing historical data about their behaviour, collected on equipment that they own, outside of that infrastructure.

In some instances, the nature of a data asset and its potential uses might oblige organisations to make it more accessible. Organisations managing data assets that stand to significantly improve lives have a duty of care to ensure it is available through public interest research or essential service provision. If the data concerns core public infrastructure – such as weather, mapping, energy, transport and health – or stands to enable powerful new discoveries, then there is a responsibility to examine any and all ethical implications. This idea underpins the 1996 Bermuda Principles for the Human Genome Project, which argued genomic data 'should be freely available and in the public domain, in order to encourage research and development and to maximise its benefit to society'.[50]

Data ethics frameworks should prompt debate about the potential creation of data monopolies and encourage open debate as to whether they are necessary or appropriate for the particular context.

Data use

The purpose of a data service or use

Some data analytics services can have negative impacts on certain demographics. Data about a person's online browsing habits, their geographical location and social media interactions are frequently used for targeted advertising, including to the most vulnerable. Advertisements targeting people with poor credit offering payday loans, and people with limited job opportunities being offered expensive courses at for-profit colleges have been well documented.[51]

[49] http://www.climateinsights.com.

[50] Kaye, J., Keeney, C. et al. (2009). Data Sharing in Genomics: Re-shaping Scientific Practice. In Nat Rev Genet. 2009 May; 10(5): 331–335: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2672783.

[51] See for example Cathy O'Neil's 'Weapons of Math Destruction' (2016).

How people – even those not directly impacted – might perceive the purpose of a data use, even where the use is not purposefully exploitative, should be taken into account by teams navigating the ethical considerations of a project. Public opposition to reported stories of data use can drive expectations of 'ethical' organisations. Even where organisations believe that what they are undertaking is lawful and ethical – perhaps even with permission from the people their data model or service affects – others might disagree. Reflecting on how that purpose might be perceived by others helps organisations to avoid accusations of unethical behaviour will help them achieve their purpose.

Case study: Unroll.me faces backlash for its data commercialisation model

Unroll.me is a US-based startup offering a free tool for managing subscription emails. In April 2017, details included in a New York Times story about the ways in which Uber used data collected by Unroll.me for commercial intelligence caused a backlash among their users.[52] Users allow Unroll.me to access their emails and email histories as part of Unroll.me's service. Retail data analytics company and owner of Unroll.me, Slice Intelligence, sells anonymised email data from Unroll.me to businesses looking for insight into the services people access and their purchasing habits.

Despite agreeing to Unroll.me's terms and conditions on accessing their inbox tool, Unroll.me users and potential users were seemingly unaware that their email histories were being monetised by Slice Intelligence and sold. People announced boycotts of Unroll.me on social media, sparking an apology from Unroll.me's CEO, Jojo Hedaya.[53] Hedaya noted that while Unroll.me's Terms of Service Agreement and Privacy Policy referenced these practices, they may not have been properly reviewed by customers. Hedaya committed to clearer messaging about data use in their application, on their website and in FAQs.

While the purposes for which Unroll.me used their customer data were outlined in their terms of service agreement, this did not alter the perception that their behaviour was unethical, when news of how Unroll.me data was used by Uber came to light. The root of this perception was a sense that Unroll.me did not clearly disclose to their users how email data would be used and who would have access to it. Unroll.me may have assumed that these uses were acceptable to users based on the terms of service.

[52] https://mobile.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html.
[53] http://blog.unroll.me/we-can-do-better.

Taking into account how a use of data may be perceived, even where permission for that use had been sought, can help organisations navigating the boundaries between ethical and unethical use.

In many instances, it will be hard to determine with certainty whether the purpose for a data service, model or analysis is ethical. Taking into account how people might perceive it, and whether people may be harmed by it, can help organisations to identify potential areas of risk.

Manipulating people's participation in democratic processes

How information is tailored to individuals and groups online (to distort their perception and reinforce biases) is coming under increasing scrutiny. Using personal data about an individual's social network, their interests and online browsing habits to selectively present information can have damaging consequences, particularly where individuals are not aware that it is their personal data that is shaping the information they see.

It has been reported that Cambridge Analytica used data modelling and psychographic profiling during the 2016 US election and the UK Brexit referendum to segment populations and selectively provide political information. This has led the UK Office of the Information Commissioner to initiate an inquiry into data misuse in politics.[54]

Segmenting potential voters based on their interests, their geographic location and other demographic information has long been part of political practices like door knocking, mail drops and issue campaigning. It has driven the success of platforms like Nation Builder, which creates action-focused websites with causes that people can donate to[55] and organisations like Blue State Digital, who grow communities, build platforms and transform organisations for the digital age.[56] To some extent, law already shapes how politicians and political parties can engage with people in the course of elections including how they declare gifts and donations, the content and authorisation of advertising, and rules around information provision on election day. When does political advertising and audience segmentation cease being acceptable and become unreasonably intrusive? This is being actively debated, and the extent to which an organisation's use of data manipulates people's participation in essential processes like elections should be carefully considered in ethical frameworks and debates.

[54] https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexit-trump.
[55] http://nationbuilder.com.
[56] https://www.bluestatedigital.com/eu.

Biases in model design

Biases in model design – in analytics, machine learning and artificial intelligence – are becoming more apparent. The issues do not simply arise from biases in underlying data sources but also design decisions that are made while algorithms are being developed.

In 2016, the first international beauty contest judged by AI – billed as analysing ‘objective’ features, such as facial symmetry and wrinkles – identified nearly all white winners.[57] Updates to Google Photos in 2015 accidentally saw black people identified as ‘gorillas’.[58] Researchers from Carnegie Mellon University in 2015 discovered that significantly fewer women than men were shown advertisements online for jobs of over $200,000.[59]

Along with taking into account potential biases in data sources, teams undertaking data projects need to be aware of biases in how a model or AI is designed. Assumptions and biases in model design – such as that women would not be interested in high-paying jobs[60] – can shape society and lead to data sources that reinforce biases.

Responding to errors and enabling feedback

An organisations can influence whether a project is considered ethical by planning for potential errors in a data service or model, and minimising the impact of these errors. Similarly, the extent to which people affected by a model can meaningfully request feedback and appeal decisions can influence perceptions of the ethics of a service. Assessing the mechanisms an organisation has in place to detect and mitigate potential errors (and limitations such as bias), and empower people affected by their service or use, is part of the Data Ethics Canvas.

[57] http://beauty.ai.

[58] http://mashable.com/2015/07/01/google-photos-black-people-gorillas/#UwcwL02Leuqn.

[59] https://www.degruyter.com/view/j/popets.2015.1.issue-1/popets-2015-0007/popets-2015-0007.xml.

[60] https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study.

Case study: Australian welfare payments provider criticised for 20% error rate in debt model

Over Christmas in December 2016, news stories emerged of the Australian Department of Human Services's automated debt recovery notices to recipients of welfare payments from its subsidiary, Centrelink. Their system cross-referenced Centrelink payment data with Australian Taxation Office records to identify discrepancies in reported income, and issued debt notices accordingly. Prior to the fully automated service in July 2016, identified discrepancies were reviewed and verified by Department of Human Services staff before debt notices were issued. Since its introduction, more than 200,000 Australians have been issued with debt recovery notices.[61]

In response to an inquiry set up by the Australian Parliament in first quarter of 2017, the Department confirmed that in 20% of cases, people appealing their debt notices were found not to owe money.[62] Under the original model, recipients of debt notices had 21 days to appeal the stated debt. The burden of proving that a debt notice was inaccurate fell onto notice recipients.

The volume of notices issued with a relatively high error rate put pressure on Centrelink staff responding to customers appealing debt notices. Debt notice recipients reported difficulties contacting Centrelink by phone and attending offices in person.[63] In response to criticisms, the Department for Human Services extended the period for appeal from 21 days to 28 days.

In this instance, people affected by the automated system tended to be vulnerable members of the Australian population – people with disabilities, financial difficulties, and people confronting periods of hardship. Whether the Department of Human Services had adequate mechanisms in place for these people to appeal automated debt notices, and steps taken to minimise error, may be factors in determining whether the overall operation of the programme was ethical.

[61] http://www.sbs.com.au/news/article/2017/03/08/department-tells-senate-inquiry-centrelinks-robo-debt-scheme-should-stay.

[62] http://mediahub.humanservices.gov.au/media/lets-talk-about-facts.

[63] http://www.abc.net.au/news/2017-03-03/centrelink-debt-controversy-what-is-robodebt/8317764.

Rarely will datasets and models be completely free of error, bias and other limitations. How organisations respond to error and inconsistency, and the mechanisms they put in place to mitigate potential harm to people affected by their data service or use, are central to taking ethics considerations seriously.

Conclusion

Discussions of ‘ethical’ and ‘unethical’ data practice are increasing in frequency and intensity. Societies are facing various data challenges arising from issues such as bias in data and algorithm design, a lack of transparency around how personal data is monetised, concern around how personal data informs the information we see and our participation in society, and how and in what circumstances people and organisations can access data at all.

We are at the beginning of an age of services, decisions and technologies that rely on data. Debates surrounding ethical data collection, sharing and use are only a few years old, but build on a rich tradition of ethical practice in sectors like medicine, journalism, computing, environmental management, and in the laws that shape our expectations of property and information (such as data protection and IP) and of each other (such as in anti-discrimination laws).

Rather than come up with an explicit ethics code or set of ethical principles for data management, we have proposed a tool – the Data Ethics Canvas – to help organisations to identify and work through issues in their data practice that may negatively impact on individuals or society. What people perceive to be ethical and unethical use of data is rapidly evolving, and so codes of practice are likely to quickly become out of date. The Data Ethics Canvas is designed to spark debate, challenge assumptions and help organisations address potential ethics issues before they happen.

Organisations need to take responsibility for aspects of their data practice that stand to negatively affect people and society. As ethics codes continue to develop within sectors, organisations and governments, we hope that the kinds of issues covered in this paper shape the content of those codes.

Most importantly, we hope that organisations developing their own ethics codes and frameworks, and applying the Data Ethics Canvas, share their learnings and insights openly. Inviting discussion demonstrates a willingness to explore ethical obligations and engage with people on data management. Building trust and demonstrating leadership in data ethics will be crucial to successful business, governance and research in the 21st century.

Data Ethics Canvas

What are your data sources?

Name and describe key data sources used in your project, whether you're collecting them yourself or getting access from third parties.

Who has rights over your data sources?

Where did you get the data from? e.g. is it data produced by an organisation or data collected directly from individuals?

Do you have permission or another basis on which you're allowed to use this data? What ongoing rights will the data source have?

What's your core purpose for using this data?

What is your primary use case, your business model?

Are you collecting more data than is needed for your purpose?

Who could be negatively affected?

Could the manner in which this data is collected, shared, used cause harm?

- be used to target, profile, prejudice people
- unfairly restrict access (eg exclusive arrangements)

Could people *perceive* it to be harmful?

Are you communicating potential risks/issues, if any?

How are limitations and risks being communicated to people affected by your project, and organisations using data?

What channels are you using?

Are there any limitations in your data sources?

Which might influence the outcomes of your project, like:

- bias in data collection, inclusion, algorithm
- gaps, omissions
- other sensitivities

What policies/laws shape your use of this data?

Data protection legislation, IP and database rights legislation, sector specific data sharing policies/regulation (e.g. health, employment, taxation)

Sector specific ethics legislation?

Do people understand your purpose?

If this is a project/use that could impact on people or more broadly shape/impact society, do people understand your purpose?

Has this been clearly communicated to them?

How are you minimising negative impact?

What steps can you take to minimise harm? Are there measures you could take to reduce limitations in your data sources? Could you monitor potential negative impact to support mitigating activities? What benefits will these actions add to your project?

When is your next review?

When will this Data Ethics Canvas be reviewed?

How will ongoing issues be monitored?

Are you going to be sharing this data with other organisations?

If so, who?

Who will be positively affected by this project?

What individuals, demographics, organisations?

How will they be positively affected?

Do they know and understand how they are positively affected?

How can people engage with you?

Can people affected appeal or request changes to the service? To what extent?

Are the appeal mechanisms reasonable?

What are your actions?

What steps are you going to take prior to moving forward with this project?

theodi.org

AUGUST 2017

Appendix

Data Ethics Canvas user guide

The Data Ethics Canvas is based on the Ethics Canvas,[64] a higher-level framework for assessing the ethical implications of any project developed by the ADAPT Centre for Digital Content Technology. The ADAPT Centre's ethics canvas is itself based on the original Business Model Canvas by Alex Osterwalder.[65] The Data Ethics Canvas will continue to evolve with user testing and feedback. For example, its format may change: it may become an interactive online tool, a print-out or series of cards.

The Ethics Canvas:

- focuses on the **people and communities affected**, ways in which they might be affected and steps to mitigate impact
- is designed to prompt **discussion and critical thinking**, enabling identification of potential areas of risk and evaluates impact in context
- considers that one type of **data activity can have lots of outcomes** (and potential consequences), depending on the context within which the activity takes place, its purpose and the organisation involved. It goes beyond being a checklist for compliance

Why use the Data Ethics Canvas

- It helps **identify and discuss potential ethics issues** arising from an organisation collecting, using and sharing data as a team
- It is a **flexible tool**, designed to tease out potential risks without predisposing an outcome and can sit alongside more formal ethics guidelines
- It will **increase the positive impact of your work** by raising issues and considerations that help to design better products and services, and reduce bias

[64] https://www.ethicscanvas.org.
[65] https://strategyzer.com/canvas/business-model-canvas.

When should organisations consult the Data Ethics Canvas?

- At the start of a project and **throughout the project lifecycle** to help identify potential ethical concerns, and as a tool to aid decision-making when changes are made
- Projects where data collection, use or distribution are **likely to impact individuals or wider society**
- Projects involving **any type of data**, regardless of whether it is open, shared or closed data, personal or non-personal

When using the canvas organisations should take into account various aspects of data practice:

- How data is **collected**
  - Information that is included and excluded
  - Design of methods of data collection
  - Accuracy and trustworthiness of data sources
  - Circumstances in which data was collected
- How data is **shared**
  - Individuals and organisations with access to data
  - Individuals and organisations excluded from accessing data, or restricted in how they may use data
- How data is **used**
  - Design of models and algorithms
  - Manipulative data presentation
  - Purpose of use
  - Margin for error

The case studies researched in this paper help to navigate these aspects of data practice, identify potential ethical concerns and decide on an appropriate course of action.

Since the Data Ethics Canvas is not a checklist, it does not offer many clear-cut answers for teams about whether their particular project or use might be unethical. Often, it is the context within which a data project takes place – the people or communities affected, how they are affected and the steps the organisation takes to minimise harm – that determine whether that organisation has behaved ethically. The Data Ethics Canvas helps organisations take responsibility for the potential impacts of their data practices on people and society.

Implementing a Data Ethics Canvas within an organisation or sector

Where a data practice has the potential to adversely impact on individuals or society, or could be perceived by the public to have an adverse impact, completing the Data Ethics Canvas should be encouraged. We have placed emphasis on 'impact' to distinguish data models and services that directly and indirectly shape our lives from internal or nonconsequential activities.

Making completion of a Data Ethics Canvas mandatory within an organisation for these kinds of projects helps to establish good practice, prior to any formal regulation. It demonstrates an organisation's commitment to treating data ethically.

There is precedent for a decision-making tool like the Data Ethics Canvas in other data regulatory areas. Under the EU General Data Protection Regulation (GDPR), the completion of a Data Protection Impact Assessment (DPIA) is mandatory for organisations where data processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 35). Article 35(3) goes on to highlight specific circumstances in which a DPIA will be required, including where extensive personal information about a person is analysed and used as the basis of decisions which have legal effects or otherwise significantly affect that person.

The substance of a DPIA resembles the substance of Privacy Impact Assessments (PIA), which the UK Office of the Information Commissioner recommends organisations processing personal data undertake.[66] While PIAs in their present form in the UK are not mandatory, the Office of the Information Commissioner can direct organisations to conduct PIAs.[67] At a minimum, DPIAs under the GDPR must include:

- a systematic description of processing operations and purpose of processing
- an assessment of the necessity and proportionality of processing operations in relation to the described purpose
- an assessment of risks to the rights and freedoms of data subjects
- measures taken to mitigate risks and ensure compliance with the GDPR

[66] https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.
[67] Ibid.

DPIAs act as a decision-making tool for data processors and controllers under data protection laws in the same way the Data Ethics Canvas is designed to function for broader ethical considerations. The canvas requires:

- a description of the data project, model or practice and its purpose
- identification of people likely to be affected by the activities
- an assessment of potential risks and limitations associated with the activities, which could negatively affect people and society
- steps taken to mitigate those risks and limitations

Impact assessments which consider the purpose of a project, its risks and potential adverse impacts and ways of mitigating those impacts exist in multiple countries – the Data Ethics Canvas could be made mandatory and subject to review.

We recommend that when the Data Ethics Canvas is completed, it is made shareable with individuals or groups affected by the particular data practice at their request and, where possible, more openly, including on public-facing websites.

ODI