Embracing Innovation in Government

GLOBAL TRENDS 2020

OECD BETTER POLICIES FOR BETTER LIVES

OPSI Observatory of Public Sector Innovation

مركز محمد بن راشد للابتكار الحكومي
MOHAMMED BIN RASHID CENTRE FOR GOVERNMENT INNOVATION

WORLD GOVERNMENT SUMMIT

Public Provider versus Big Brother

NOVEMBER 2020

TRENDS.OECD-OPSI.ORG

#SALMANQADIR

OECD
BETTER POLICIES FOR BETTER LIVES

OPSI Observatory of Public Sector Innovation

مركز محمد بن راشد للابتكار الحكومي
MOHAMMED BIN RASHID CENTRE FOR GOVERNMENT INNOVATION

WORLD GOVERNMENT SUMMIT

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

#SALMANQADIR

Table of Contents

OPSI Observatory of **Public Sector Innovation**

OPSI serves as a global forum for public sector innovation, helping governments to understand, test and embed new ways of doing things through the application of fresh insights, knowledge, tools and connections.

- oecd-opsi.org
- @OPSIgov
- opsi@oecd.org
- oe.cd/opsinewsletter

مركز محمد بن راشد للابتكار الحكومي
MOHAMMED BIN RASHID CENTRE FOR GOVERNMENT INNOVATION

MBRCGI works to stimulate and enrich the culture of innovation within government through the development of an integrated innovation framework. The goal is for innovation to become one of the key pillars of the UAE government with the aim of developing government operations and enhancing competitiveness to make the UAE one of the most innovative governments around the world.

- mbrcgi.gov.ae
- @mbrinnovation
- info@mbrcgi.gov.ae

Introduction

The OECD Observatory of Public Sector Innovation (OPSI) and the United Arab Emirates (UAE) Mohammed Bin Rashid Centre for Government Innovation (MBRCGI) have spent the last year conducting research and analysis to understand how governments and their partners are innovating to cope with rapid change, increasing complexity and uncertainty, accelerating technological transformation and ever-increasing demands from the public. As part of the MENA-OECD Governance Programme,[1] we have conducted extensive research and held a global Call for Innovations crowdsourcing exercise to surface key innovation efforts[2] and met with innovation teams from around the world to hear their stories (Figure 1). Many of the cases identified through this work are included on OPSI's public Case Study Platform.[3]

Figure 1: Crowdsourcing and research to surface trends and cases

Through this work, OPSI and the MBRCGI have found that governments are taking exciting and innovative actions to transform themselves. Throughout 2020, OPSI and the MBRCGI are issuing a series of five report on 2020 trends in public sector innovation,[4] which will culminate in the launch of the final report at OPSI's two-day virtual event *Government After Shock: An unconventional event for unconventional times* on 17-18 November 2020.[5] The trends surfaced for 2020 build upon and demonstrate the evolution of the remarkable efforts detailed in our previous Global Trends series of report.[6]

The first report for 2020, published in July, detailed key themes for *innovative responses to the COVID-19 crisis*, which continues to unfold and presents countless and cascading challenges. In September, the second report found that while governments continue to grapple with COVID-19, they are taking action to bring about *seamless government* by innovating to eliminate points of friction with those they serve and actively shaping tomorrow's possibilities with action today. In October, the third report in the series explored the issues of *focusing on the overlooked*, and how governments are using innovative approaches to provide new opportunities for disadvantaged and underserved groups.

1 https://oe.cd/mena-gov.

2 https://oecd-opsi.org/call-for-innovations-2020.

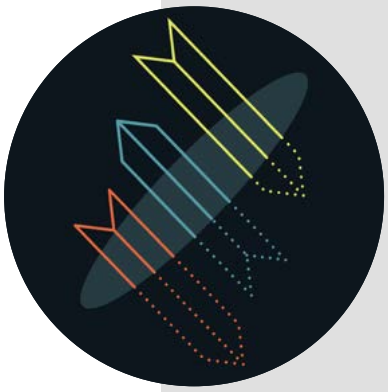
3 https://oecd-opsi.org/innovations.

4 Each report and an accompanying digital story are published at https://trends.oecd-opsi.org.

5 See https://gov-after-shock.oecd-opsi.org. All innovators are invited to participate.

6 The reports for 2017-2019 are available at https://oe.cd/innovationtrends.

For the fourth report in this series, OPSI and the MBRCGI's research explores the powerful new technologies and opportunities that governments have at their disposal to let them better understand the needs of citizens. The research shows that governments must be cautious in exploring these possibilities and should leverage them in ways that do not undermine public trust. Governments need to balance the tensions of using data harvesting and monitoring, and technologies that can identify individuals, to serve the public interest, with the inevitable concerns and legitimate fears about "big brother" and risks of infringing on freedoms and rights. Through the lens of navigating *Public Provider versus Big Brother*, innovation efforts fall into two key themes:



01 : Data harvesting and monitoring

Governments have access to more detailed data than ever before as well as sophisticated analysis and monitoring methods, techniques and devices to understand the lived experience of citizens and provide relevant services. However, such access involves risks and considerations which require serious reflection on the part of government.

02 : Biometric technologies and facial recognition

A range of facial and body recognition and other biometric tools offer opportunities to provide easy access to tailored services, as well as the unprecedented ability to identify and track individuals and gather unprecedented knowledge about their behaviours and movements.

These themes are discussed in this report alongside real-world examples and case studies.

Collecting Mobile Data About Women to Build Safer Public Transportation

CHILE

A "data collaborative" in Santiago analyses private telecoms data about where and when people make mobile phone calls, along with a range of open data and socioeconomic information, to better understand the gendered dimensions of urban mobility.

Facial Verification for National Digital Identity

SINGAPORE

Singapore is developing a biometrics system as part of their National Digital Identity programme to allow citizens to make transactions for both public and private services, such as banks, through the use of facial verification rather than passwords or physical ID cards.

Designing a Biometric Policy for Humanitarian Aid

INTERNATIONAL COMMITTEE OF THE RED CROSS

As biometric projects and services continue to grow, policies governing their use are lagging behind. Accordingly, the International Committee of the Red Cross have designed their own policy, which offers a number of lessons and good practices for governments pursing their own.

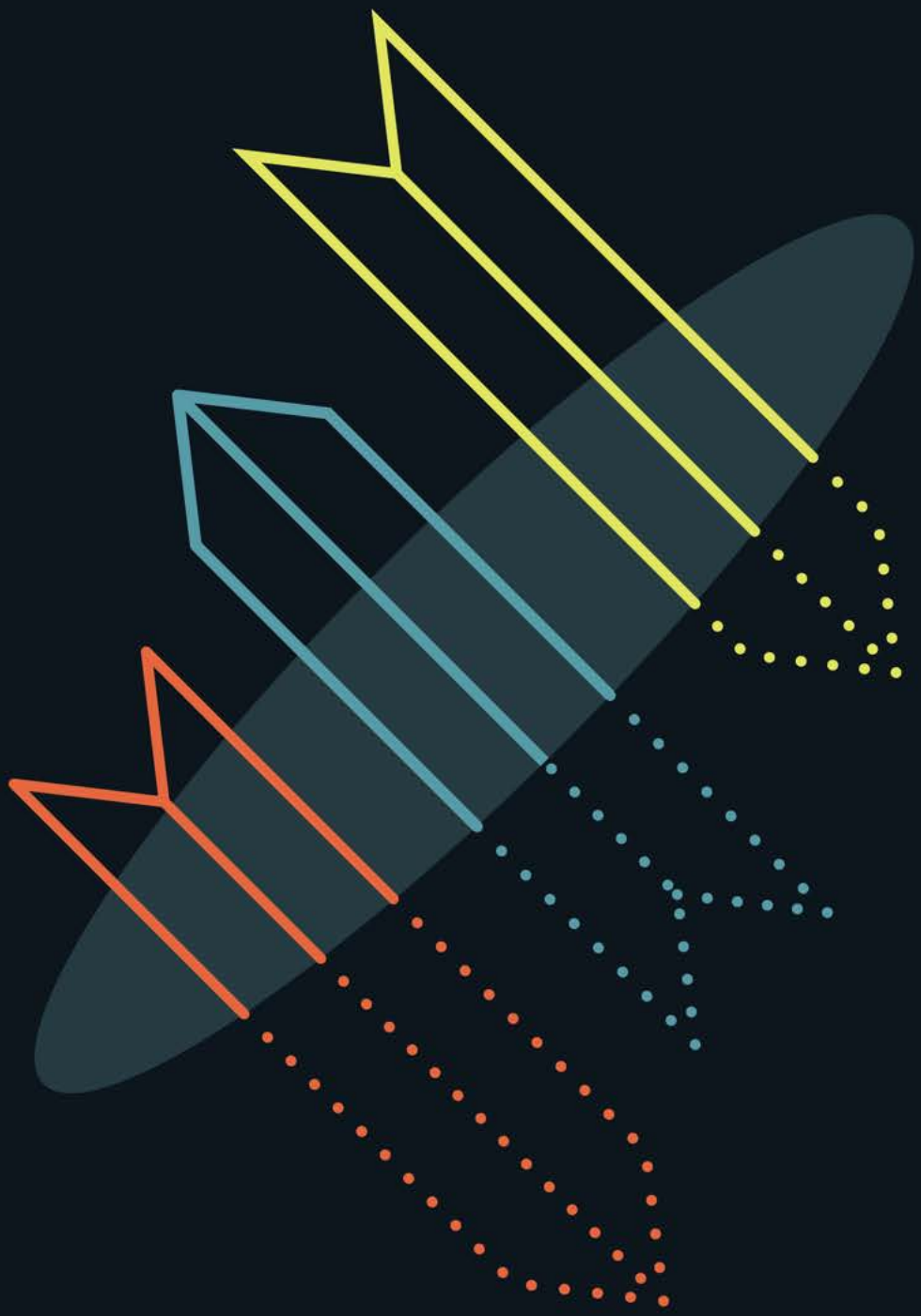
OPSI and the MBRCGI explore these and other efforts in what is a challenging and evolving field, with the aim of aiding others in their learning and testing of these contentious issues. Governments need to engage with these new opportunities but must equally be aware of the limits of citizens' tolerance and the dangers involved in accelerating too far, too fast without the necessary safeguards.

As a result of this work, OPSI and the MBRCGI have developed three key recommendations to help guide governments in exploring the use of technology to collect new types of data and insights:

1. Actively engage with the issues raised by these technologies.
2. Prioritise earning trust from the public in order to successfully implement services that leverage these technologies.
3. Work collaboratively across national borders in order to understand the limits, pitfalls and opportunities of these technologies.

KEY THEME 01

Data harvesting and monitoring



Data are fundamental to effective and efficient government and the digital transformation of the public sector. Data underpin the provision of programmes and services, allowing governments to verify identities and distribute benefits based on eligibility criteria; data enable the monitoring and maintaining of natural and environmental resources; data form the core of policy research, ensuring sound and evidence-based decision making; and data are central to understanding, reporting on and improving operations and outcomes. For this and other reasons, the OECD (2020a, 2019a, 2019b, 2017) and governments around the world have recognised data as a strategic asset, the value of which increases when easily accessed, shared, used and re-used, as appropriate.

As the COVID-19 pandemic has demonstrated, governments have a genuine need to know what is happening and who is doing what and to whom in real time. Various technologies and techniques can provide a rich source of data for governments, particularly those that enable monitoring in different forms. The full capabilities and potential of some of these technologies and techniques are still being discovered, and their strengths, drawbacks and other considerations are being explored by the public sector. Likewise, there are strong civil society concerns about overreach or the risk of breaching personal privacy and liberties. Can governments navigate this uncertain terrain and use new technologies effectively to discern and deliver what is needed and expected of them, without stepping into "Big Brother"[7] territory?

Data harvesting

A digital world produces an incredible amount of data, as interactions and behaviours are captured by mobile devices and other sensors, providing insights into every aspect of people's lives. The continued growth of the Internet of Things[8] will only magnify this trend, as even mundane activities start to provide potentially significant data about people and their behaviours. Data harvesting, thus, can provide governments with important insights into real-time events, trends and behaviours on the ground. It can also help explain why things are happening in a particular manner. As the case study on "Collecting mobile data about women to build safer public transportation", presented later in this report, demonstrates, data harvesting can reveal the extent of problems that might otherwise have gone undetected or proven difficult to map – in this case, variations in the use of public transport by men and women. Armed with such insights, governments can devise interventions to address identified issues and challenges.

Data harvesting can also be a valuable tool during or after emergencies, as governments try to assess the extent of impacts on a population. This is particular important in terms of delivering timely responses or assistance, especially in the case of disaster relief. Rapid information feedback loops are crucial to make good decision making in urgent situations. A recent study observed the use of a number of new big data sources in disaster relief, including satellite and aerial imagery, drone videos, sensor web networks and the Internet of Things, spatial data, crowdsourcing, real-time social media, and mobile GPS and telecoms data (Yu, Yang and Li, 2018).

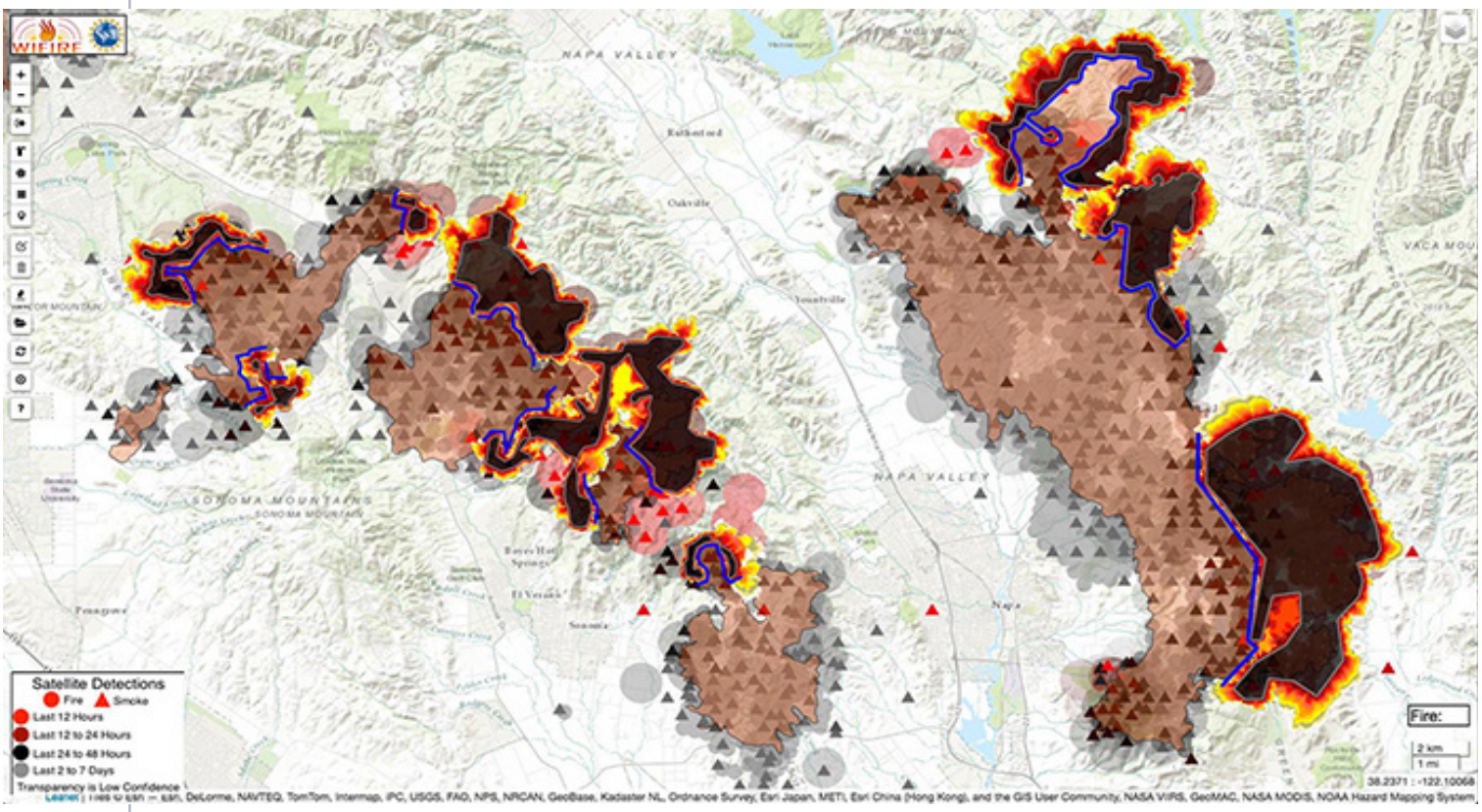
This trend has become particularly apparent in recent years with regular wildfire disasters in North America (BBC News, 2020), Australia (Givetash, 2020) and even the Arctic Circle (Witze, 2020). In California, US, the city of Los Angeles has been using big data analytics to assist their response in real time. The Fire Department partnered with the San Diego Supercomputer Center and their WIFIRE Lab to develop a programme capable of making predictions about where fires would spread, using information about local geography, weather conditions and potentially flammable materials, all gathered from government data sets and local sensors (Del Real, 2019). The WIFIRE Firemap is described by its creators as a "decision-support and information tool", and is used as such, helping to make predictions instantly, by combining data sets and analytical techniques, and modelling them on a public platform (see Figure 2). Its popularity during wildfires in 2018 led to broader usage by other fire departments and national government support for the tool.[9]

7 https://en.wikipedia.org/wiki/Big_Brother_(Nineteen_Eighty-Four).

8 www.oecd.org/going-digital/mdt-roadmap-measuring-internet-of-things.pdf.

9 See also the uses of data harvesting in the first 2020 innovation trends report, *Innovative Responses to the COVID-19 Crisis*, at https://trends.oecd-opsi.org.

Figure 2: WIFIRE's Firemap platform showing a fire outbreak in Napa Valley



Source: https://ucsdnews.ucsd.edu/pressrelease/northern-ca-wildfires-generate-1.5-million-views-of-uc-san-diegos-firemap.

Taking the predictive approach even further, Portland, Oregon, created a Fire and Rescue Blueprint for Success,[10] based on the emergent understanding that the main deaths by fires in cities do not occur as a result of large conflagrations engulfing skyscrapers and neighbourhoods, but are actually small events associated with social, health and economic status. As such, the city is using data on poverty, blight, drug addiction, mental health and homelessness as part of their ambitious plan to reach zero deaths from fire.

Such analytics can have a wide range of uses. A study from Deloitte describes a number of examples of governments around the world using data harvesting and analytics to identify, understand and attempt to address more long-term, complex problems. For example, Luton Borough Council, located just outside of London, has been using data modelling to identify individuals in the borough at greater risk of homelessness. By combining income and other financial data, and focusing on risk factors, the council was able to identify low-income households – or, specifically, those with low financial resilience. By correlating these findings with other socio-demographic data, the council can effectively model the impacts of new policies, such as the Universal Credit scheme, and determine how they would affect certain households, thereby enabling them to track and target those households to provide preventative assistance (Alvarez Vilanova, 2018). Moving beyond passively gained insights on current status, data harvesting can help governments simulate and model the potential effects of their policies and other interventions. The use of data for anticipating and planning is discussed in the OECD report *The Path to Becoming a Data-Driven Public Sector* (OECD, 2019a).

Data harvesting can also help people better understand their own lives and the environment in which they live. Harvesting a wide range of data and making them accessible and relevant can help better inform people about issues affecting their quality of life, and perhaps lead them to make different decisions and choices (see Box 1).

10 www.portlandoregon.gov/fire/77452.

Box 1: The HOPE project

The HOPE project in Helsinki aims to produce a comprehensive hyper-local air quality monitoring network including crowdsourced portable monitors that give citizens air quality information on exposure to air pollution in the places where they live and travel in the city. The project focuses on three districts in Helsinki that experience various air quality challenges. The first major milestone of the HOPE project is the planning and building of three state-of-the-art local monitoring networks in these areas.

In addition to building monitoring networks, the project has launched crowdsourced campaigns for mobile sensor devices to measure air quality. Up to 100 citizens at a time will carry the devices which will produce hyper-local, real-time air quality data, which can be processed as a part of regional air quality information, maps and forecasts. State-of-the-art technologies developed through the project, such as AI algorithms, machine learning and edge-computing, are used in calibrating the sensors and crunching the data.

Source: https://oe.cd/hope-project, https://ilmanlaatu.eu.

As governments not only gain access to richer and more sophisticated data through different means of data harvesting, there will be opportunities to better understand the service delivery context and the factors shaping the policy environment.

Monitoring and surveillance

Related to and often building upon data harvesting, advancements in technology are also providing governments with more powerful abilities to survey real-time events through monitoring and surveillance. Surveillance, defined by Lyon (2007, p. 14) as "any focused, routine or systematic attention to personal details, for the purpose of control, influence or management", is becoming easier to conduct, and so perhaps, unsurprisingly, more common. As Lyon notes, surveillance is endemic to the modern state and constitutes a key feature of bureaucratic administration for purposes such as tracking compliance. However, surveillance also has negative connotations, with the word itself prompting a visceral reaction among some. This is especially true where it is perceived as veering into areas of control and influence rather than the more mundane area of management.[11] Nonetheless, monitoring and surveillance efforts are growing in government, warranting a discussion and focus on the topic.

A common manifestation of modern day surveillance is the use of cameras, particularly closed-circuit television (CCTV). Some cities have introduced cameras in large number to provide a sense of safety and to try to prevent and track crime. Given their proliferation, OPSI does not consider video monitoring and surveillance activities to be innovative. However, the implications and possibilities of video surveillance take on a new dimension when such cameras are mounted on a drone. Real-time surveillance with drone scouts allows first responders to gain access much faster to information about potential incidents and better assess the needed response, potentially saving time and delivering more effective outcomes (see Box 2). Louisville, Kentucky is also experimenting with drone-based incident response.[12] OPSI and the MBRCGI observed a noticeable uptick in drone programmes in this year's research and Call for Innovation. Some governments have issued specific guidance on drones and their relation to privacy principles – one example being the guidance developed by Queensland, Australia.[13] The European Union has provided funding to Drone Rules, an awareness-raising campaign and online course on drone laws and regulations across the European Union, including a code of conduct and privacy rules. Drone Rules also released specific guidance on aligning drone usage with the General Data Protection Regulation (GDPR).[14]

11 It is important to note the distinction, on the one hand, between smaller-scale monitoring and surveillance activities that seek to improve general public safety and the efficiency and effectiveness of government policies and services, and, on the other, government surveillance programmes that seek to protect national security. OPSI's current portfolio of work and expertise does not include national security or the organisations and agencies that support this field, and data harvesting or surveillance programmes that fall in this area do not fall within the scope of this report.

12 https://oe.cd/air-incident-response.

13 https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/drones-and-the-privacy-principles.

14 See https://dronerules.eu/assets/covers/DroneRules_factsheet_0vf.pdf.

Box 2: Chula Vista police drone as first responder

The Chula Vista, CA Police Department (CVPD) in San Diego, US, routinely deploys drones to respond to emergency calls and provides incident management and a live video feed to officers. This live video, or Decision Quality Data (DQD), gives first responders critical information enabling them to plan their tactical response to an emergency. During the pilot study, drones were launched from two sites and could fly within a geo-fenced area (including minimum and maximum altitudes). The drones typically arrive between 2-3 minutes from launch, often beating ground units. The department's two commercial drones are equipped with a 30x zoom camera, providing powerful zoom capability. As first responders are often the least experienced personnel, the drone as first responder approach changes how the police force potentially responds by allowing for more experienced people to observe the response and make corrections or re-prioritise resources in real-time.

Source: https://oe.cd/drone-responder.

Combining technological approaches

As in many other fields, real potential lies in a combination of technologies, widening the opportunities for more sophisticated surveillance. Through the lens of "AI surveillance", Steven Feldstein, an expert research on the intersection of advanced technologies and governance (2009), identifies new techniques promising greater power (and potential problems) (Table 1).

Table 1. Summary of AI surveillance techniques and global proliferation

AI Surveillance Technique	Description	Global Proliveration (out of 75 countries)
Smart Cities/Safe Cities	Cities with sensors that transmit real-time data to facilitate service delivery, city management, and public safety. Often referred to as "safe cities," they incorporate sensors, facial recognition cameras, and police body cameras connected to intelligent command centers to prevent crime, ensure public safety, and respond to emergencies. Only platforms with a clear public safety focus are incorporated in the index.	56 countries
Facial Recognition Systems	Biometric technology that uses cameras (still images or video) to match stored or live footage of individuals with images from databases. Not all systems focus on database matching; some systems assess aggregate demographic trends or conduct broader sentiment analysis via facial recognition crowd scanning.	64 countries
Smart Policing	Data-driven analytic technology used to facilitate investigations and police response; some systems incorporate algorightmic analysis to make predictions about future crimes.	53 countries

Source: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

One case of matching AI surveillance with data harvesting comes from a group of researchers at George Washington University, Temple University and Adobe in the United States, which together built a large dataset containing over a million images from 50 000 hotels across different countries. The researchers hope that their public Hotels-50K dataset will help developers train neural networks to determine the location of potential victims of human trafficking, by matching the backgrounds in photos from online ads with specific hotel rooms within seconds.[15] When datasets are combined with algorithm-enabled surveillance, new possibilities emerge.

15 www.theregister.com/2019/02/05/ai_human_trafficking.

Of course, such technologies may not always work as intended or be reliable at first (or perhaps ever). For instance, also in the United States, a range of cities have adopted ShotSpotter technology, which uses sensors to attempt to detect gunshots in different locations. However, the benefits are not necessarily clear-cut as of yet, with examples of police officers responding to false alarms.[16] As in many other fields, and especially with emerging technologies, the promises of surveillance technology can extend beyond initial capacity to deliver.

There is a risk also of viewing monitoring or surveillance activities through a single lens, without regard for its more systemic effects and consequences. For instance, while CCTV has been found to have a modest but real impact on reducing certain types of crime (mostly related to the drug trade, property and vehicles), numerous conditionalities must be taken into account (e.g. whether monitoring is passive or active shapes response times).[17] In addition, there are potential concerns, particularly around privacy and how the data are used. [18] The usefulness of a tool to address a particular problem needs to be weighed against other, broader concerns. The example of China's social credit scores demonstrates the highly controversial and intentional effects of combining different types of digital data collection and monitoring tools (see Box 3).

Box 3: China's social credit scores

In a number of Chinese cities, there are ongoing trials of a social credit system that can influence access to services, credit, jobs and travel based on the apparent "trustworthiness" of the citizen. The system that determines a social credit score is powered by AI, and includes facial recognition technology linked to CCTV surveillance (see the facial recognition discussion later in this report), data collection from smartphone apps to measure online behaviour, financial assets and government records relating to education and medical and state security assessments.

This gives the authorities the ability to control and shape the behaviour of citizens. What someone says, purchases and who they associate with can influence their ability to participate in public life. This can have a chilling effect on dissent and scrutiny of the state.

This type of social credit system is technologically feasible in many countries through the aggregation of individuals' data from diverse sources, but that does not mean it is either desirable or inevitable. Whether such systems emerge, and what controls they are subject to, are significant political questions. The answers may in part depend on cultural norms and the balance afforded to the importance of a stable and safe society, or privacy and individual freedom. Legal and policy standards can also foster or hinder these types of activities, as discussed in the next section of this report.

Source: www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digitaldictatorship/10200278, https://datajustice.files.wordpress.com/2018/12/data-scores-as-governanceproject-report2.pdf and https://time.com/collection/davos-2019/5502592/china-social-credit-score.

Nonetheless, monitoring and surveillance efforts that leverage one or more traditional, emerging or not-yet-in-existence technologies will continue to grow. This is consistent with history, and will likely introduce many grey areas and ethical dilemmas which will need to be fully considered and evaluated. Governments have a significant role to play in determining the norms and rules around the use of such technologies, in terms of use within the public sector and among broader society and the economy. Box 4 presents a historical overview of the progression of monitoring and surveillance, and seeks to demonstrate how shaping norms is vital to guiding the use of these technologies.

16 www.voiceofsandiego.org/topics/public-safety/shotspotter-sensors-send-sdpd-officers-to-false-alarms-more-often-than-advertised.

17 https://onlinelibrary.wiley.com/doi/full/10.1111/1745-9133.12419.

18 www.aclu.org/other/whats-wrong-public-video-surveillance.

Box 4: The introduction of monitoring and surveillance through economic and performance pressures

There is a long history of organisations working to improve their performance through increased awareness of workflow dynamics and trends both internally and, to some extent, externally. For instance, Taylorism, or "scientific management", which originated in the late 1800s, was rooted in the belief that labour productivity could be enhanced by identifying each step of industrial workflow through time and motion studies, and having managers impose the resultant insights on staff. More recently, approaches such as "lean", total quality management and "agile" aim to aid continuous learning and drive greater efficiencies. Technology gives managers new ways to monitor their employees, sometimes with the support of their governments. While this does not always constitute surveillance, there are examples of organisations trying to leverage new technologies in this spirit.

To take one example, in 2014, the State Grid Zhejiang Electric Power Company introduced brain surveillance devices to monitor wearer's brainwaves in order to help train new employees and reduce mistakes. While there are debates about the extent to which such devices can provide useful and meaningful data and insights, their usage underscores the likelihood that monitoring and surveillance will have a range of economic as well as social and political dimensions. A more mundane example is the tracking apps used by some US universities to trace the movement and location of students during COVID-19 pandemic. In the absence of strong societal expectations and norms and/or government regulation and limits, there are likely to be economic and other pressures for organisations to introduce such technologies, which may then leak into other spheres of life.

Source: www.mindtools.com/pages/article/newTMM_Taylor.htm, www.scmp.com/news/china/society/article/2143899/forget-facebook-leak-china-mining-data-directly-workers-brains; www.theverge.com/2018/5/1/17306604/china-brain-surveillance-workers-hats-data-eeg-neuroscience and www.theatlantic.com/technology/archive/2020/09/pandemic-no-excuse-colleges-surveil-students/616015.

Limitations and pitfalls to consider

Data harvesting and monitoring and surveillance are powerful approaches that can uncover significant information that might otherwise have been ignored, missed or dismissed. However, use of this power is not without legitimate concerns, and due care needs to be taken. Data harvesting and surveillance can provide unparalleled insight into people's individual and collective lives and it would be naïve to think that the results of these tools will always be uniformly positive.

With a focus on leveraging these solutions and methods for public sector transformation and innovation, the OECD report, *The Path to Becoming a Data-Driven Public Sector* (OECD, 2019a),[19] explores some of these issues and identifies a need for governments to pay more attention to data ethics, privacy and consent, transparency and security, if they are to secure and maintain citizen trust in the usage of personal and collective data. Correctly handling data can balance innovation with ethical data practices, while placing users at the centre of the product and service design process. For this to happen, citizens need to understand how data about them is being collected, analysed and stored and how long it will be kept for, so the citizens see the value created from their input, as well as the values and culture of the government handling the data" (OECD, 2019, p. 105).[20] Governments thus need to prioritise data governance so that citizens can have trust in their governments to use their data for public value. Figure 3 outlines key aspects that governments should evaluate when considering such approaches, the specifics of which are covered in-depth in the above-mentioned report. In addition, the OECD is currently finalising a set of "Good Practice Principles" that may help governments as they think through considerations for data harvesting and use (Box 5).

19 The work of the OPSI and the MBRCGI focuses on public sector innovation and the ways that governments can take action to transform their internal operations, policy-making processes and service delivery. This focus shapes the scope of this report; however, governments also play many other roles with regard to these areas. One of the most important of these is the role of a regulator for non-governmental actors. The OECD Regulatory Policy Division, which forms part of the Public Governance Directorate (GOV), works with member and non-member countries to support the implementation of good regulatory practices. See www.oecd.org/gov/regulatory-policy for additional work and research in this area, including on regulatory policy related to technology solutions.

20 https://www.oecd-ilibrary.org/governance/the-path-to-becoming-a-data-driven-public-sector_059814a7-en.

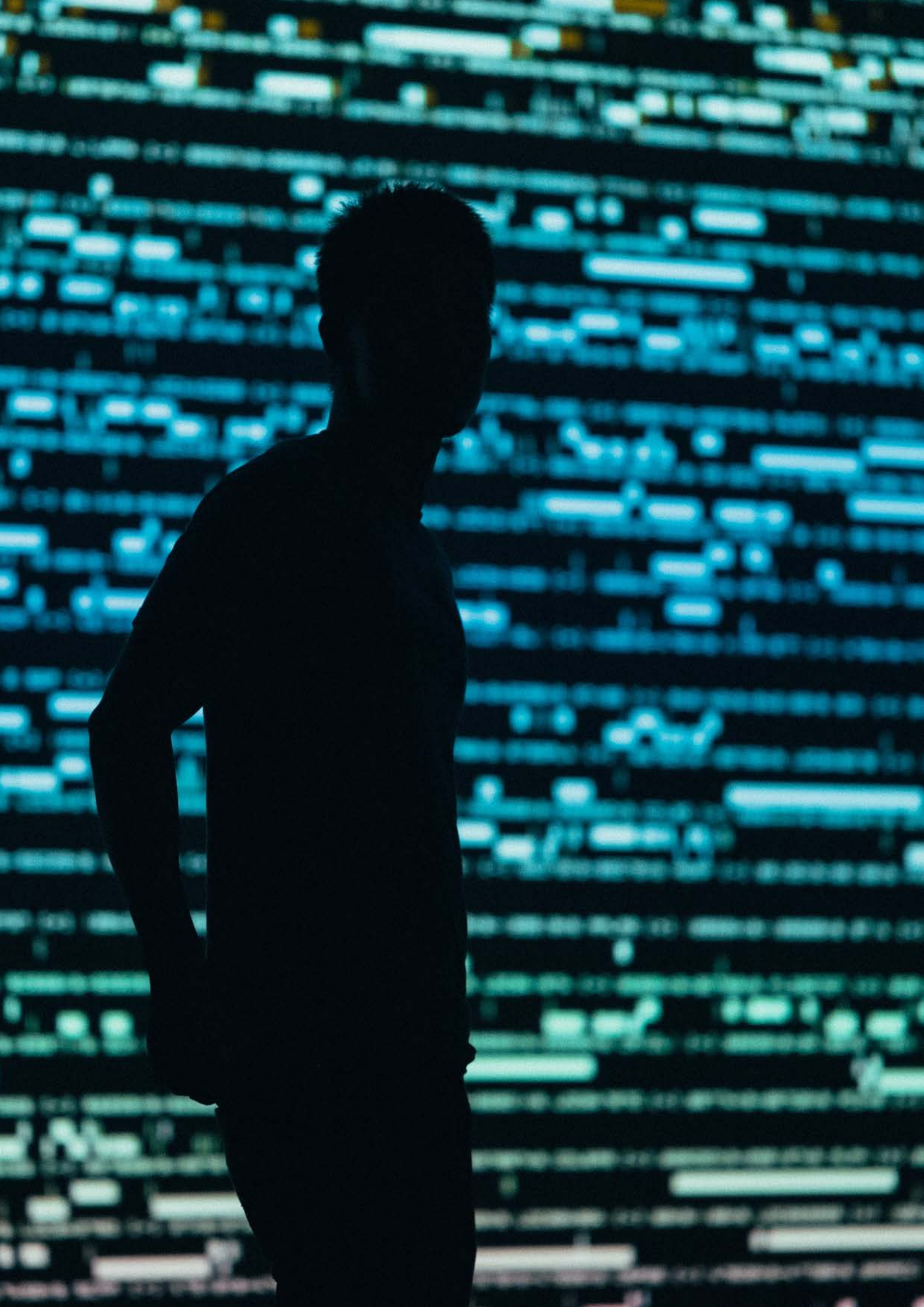
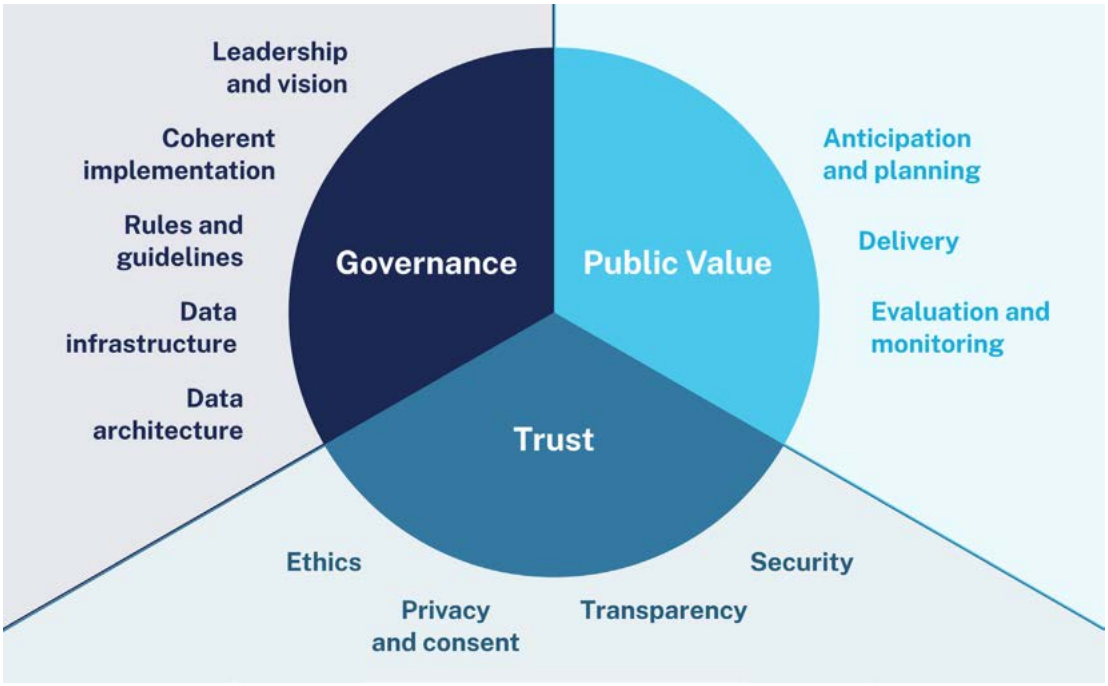


Figure 3: The 12 facets of a data-driven public sector



Source: www.oecd.org/gov/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm.

Box 5: Draft OECD Good Practice Principles for Data Ethics in the Public Sector

Governments need to be prepared to handle and address issues and concerns associated with data corruption; biases in data generation, selection and use; data misuse and abuse; and unexpected negative outcomes derived from data use increase. This includes biometric data and associated applications. The OECD Digital Government and Data Unit is in the final stages of drafting guiding principles on data ethics to help government, the draft principles of which are listed below. When published, each will include additional context and details for public sector actors.

- Use data with integrity.
- Be aware of relevant arrangements for trustworthy data access, sharing and use.
- Incorporate data ethical considerations into governmental, organisational and public sector decision-making processes.
- Safeguard the agency of data users to intervene in automated decision-making processes.
- Be specific about the purpose of data use, especially in the case of personal data..
- Define boundaries for data collection, access, sharing and use.
- Be clear, inclusive and open.
- Broaden individuals' and collectives' control over their data.
- Be accountable and proactive in managing risks.

Source: OECD (forthcoming). To be published soon at https://oe.cd/digitalgov.

The OECD has also developed key recommendations for privacy and data protection in this area, including data harvesting efforts to fight COVID-19, which has rapidly accelerated the use of data harvesting and monitoring techniques (Box 6).

Box 6: Key recommendations for data privacy and security

Data collection and monitoring solutions should be implemented with full transparency, in consultation with major stakeholders, robust privacy-by-design protections and through open source projects (where appropriate). Governments should consider:

- The legal basis of the use of these technologies, which varies according to the type of data collected (e.g. personal, sensitive, pseudonymised, anonymised, aggregated, structured or unstructured).
- Whether the use of these technologies and the subsequent data gathering is proportionate, and consider how the data is stored, processed, shared and with whom (including what security and privacy-by-design protocols are implemented).
- The quality of the data collected and whether it is fit for purpose.
- Whether the public is well-informed and the approaches adopted are implemented with full transparency and accountability.
- The time period within which more invasive technologies that collect personal data may be used to combat the crisis. Data should be retained only for so long as is necessary to serve the specific purpose for which they were collected.

Privacy-by-design seeks to deliver the maximum degree of privacy by ensuring that personal data protections are built into the system, by default. Privacy-by-design may, for example, involve the use of aggregated, anonymised or pseudonymous data to provide added privacy protection, or the deletion of data once their purpose is served.

Source: https://oe.cd/privacy-apps-biometric.

As an increasing number of these approaches leverage Artificial Intelligence, governments should also ensure that they adhere to the OECD Principles on AI, which have been recognised by all OECD countries and a number of non-member states (Box 7).

Box 7: Principles for the responsible stewardship of trustworthy AI

- AI should benefit people and the planet by driving inclusive growth, sustainable development and wellbeing.
- AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.
- There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
- AI systems must function in a robust, secure and safe way throughout their life cycles, and potential risks should be continually assessed and managed.
- Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.

Source: https://oecd.ai

Governments should also be wary of the claims of any new technologies. While many new technologies take time and investment to reach their potential and deliver on their promises (and of course some never will), there can be clear risks from the outset that need careful consideration. Governments should not let this serve as a disincentive, however; rather, they should dedicate resources to fully understanding these issues. Governments should explore the use of data harvesting and appropriate monitoring and surveillance efforts, as taking a "wait and see" approach can lead to missed opportunities to attain new levels of insight.

Lastly, it should be recognised that citizens often react negatively if technology is introduced which they do not trust or appreciate. People will push back if the benefits are not clear or if there is insufficient trust in the approach. This highlights the need for governments to actively engage with these technologies to understand the implications and to maintain or gain the trust of their people.

Collecting Mobile Data About Women to Build Safer Public Transportation

Chile

Women and men move through cities differently. Studies have shown that women adapt their behaviour for a variety of reasons, including their relative fear of different spaces or types of transport. While traditional methods such as household surveys allowed researchers to ascertain how the urban mobility gap differed between men and women, new data science methodologies enable governments to visualise the urban mobility patterns of women. In Santiago, Chile, a data collaborative that brings together public and private sector experts and data scientists, has used a mixture of open data records and unique data insights from the telecoms company Telefónica, in the form of Call Detail Records (CDRs), to map the movement of 400 000 people across the city. This unique partnership combines new data sources and analytical skills to provide the deepest statistical-based insights yet into the gender mobility gap in urban spaces. This new type of analysis highlights the importance of governments taking risks and trying new things, even in the area of research. Through understanding the lives of their citizens in greater detail, governments can start to make more targeted and bespoke policy interventions for particular demographics.[21]

21 Unless otherwise indicated, the information for this case study was sourced from an interview and correspondence with Natalia Adler, former Data, Research, Policy Manager in UNICEF, Laetitia Gauvin and Michele Tizzoni, researchers from the ISI Foundation, as well as further correspondence with themselves and Ciro Cattuto, also a researcher from the ISI Foundation and senior author of the study, in September and October 2020.

The problem

The ways in which different groups use public spaces differs, and government policy making needs to take these differences into account when designing policies and services. The urban mobility of women, much like the general use of public space, is governed by women's perceptions and fear of crime as well as victimisation and harassment. Women alter their behaviour according to their relative fear of different types of transport, changing travel habits to avoid places that they associate with a potential threat (Loukaitou-Sideris, 2014). Women also undertake more multi-stop trips to perform chores – a particularly pronounced trend in societies with more concrete-cast gender roles – and also use transport differently according to their economic situation (e.g. higher paid and formal vs lower paid and informal work) (Brown, McGranahan and Dodman, 2014). This situation carries implications – without full use of transportation infrastructure, women and girls are unable to fully tap into the full economic and social opportunities that the city provides. Given the problem and its consequences, it is vital that governments design and implement policies that address this issue.

However, governments can only make informed decisions when they have the requisite information. Unfortunately – or perhaps as a result of the knowledge systems that initially produced these trends – outdated or few gender-disaggregated data have been collected on how women use urban transport (Gauvin et al., 2020), particularly in poorer countries where public organisations are under-resourced. Without specific knowledge of the problem or how to measure it, governments cannot develop the necessary solutions. However, new technologies are changing what we can measure, including for women in the area of urban mobility, as is becoming apparent in Santiago, Chile.

An innovative solution

In 2018, UNICEF researchers were working with the New York University (NYU) GovLab on a methodology to leverage large amounts of private data to solve complex social problems. These problems were selected based on different criteria ranging from their level of complexity and lack of availability of traditional data, to the existence of local champions. Using the methodology designed with GovLab, UNICEF set a problem statement defining the specific research issue, as well as the type of data needed to address it. The initiative was the first of its kind to perform such a detailed analysis of gendered mobility data, which represents a significant undertaking. To achieve this, UNICEF formed an innovative data collaborative to work through the challenges together. The collaborative was intentionally designed to bring together actors from all sectors with different skill sets, expertise and resources, along with the owners of relevant private data needed to run the project. It comprised the following key players:

- **UNICEF** was the key driver of the initiative – with inputs from the Regional Office for Latin America and the Caribbean based in Panama, including the Santiago UNICEF office, which initially identified the gendered aspects of mobility. These efforts were headed by Natalia Adler, who was UNICEF's Data, Research, Policy Manager at the time.

- The **UN Foundation** and its **Data2X** platform were the principle supporters of the collaborative's activities through a grant, as part of their Big Data and Gender Challenge.[22]

- **GovLab** contributed heavily to the co-ordination and design of the activities through their Data Collaboratives initiative.[23] These efforts were led by Stefaan Verhulst, who was the principal investigator for the Data2X grant.

- The **CRT Foundation** and the **ISI Foundation** provided research and data science capabilities and critical funding through a scholarship programme aimed at "data science for social impact" (also known as the LaGrange Scholar ships). The CRT Foundation, in particular, funded the main full-time staff person on the project, Simone Piaggesi. Ciro Cattuto from the ISI Foundation served as principal author for the study, in coordination with Laetitia Gauvin and Michele Tizzoni.

- **Telefónica Research and Development**[24] has spearheaded data sharing for social good with strong privacy guarantees and facilitated access to relevant data for the initiative, and the **Universidad del Desarollo** (UDD), which already has a relationship with Telefónica and an established framework and significant skills in place for sharing and analysing carefully anonymised data for social good. UDD (in particular, Leo Ferres) also carried out most of the con versations with local authorities, as the university is based in Santiago and had the relevant connections.

22 https://data2x.org/resource-center/gender-gaps-in-urban-mobility.

23 https://datacollaboratives.org.

24 www.tid.es.

The principal partners in the research were GovLab, which was also the primary contractor for the Data2X grant, UNICEF, with their public policy and research background, UDD researchers, who had significant and deep expertise on analysing call detail records (described below), and data scientists from the ISI Foundation, who provided additional data science and data analysis skills. UDD and ISI researchers had been working in Santiago on mobility modelling and, thus, had a good understanding of the available data. Partnerships with Telefónica's Research and Development Centre and the UDD were essential to the work. Telefónica is one of the largest telecom networks in Chile, and had already established a protocol to share their private data in a clean, anonymised format with UDD, and thus with the data collaborative.

The collaboration drew on a combination of open data and private data sources. Telefónica were able to provide anonymised private data for three months of Call Details Records (CDRs), which register every time a mobile phone call connects to a particular cell tower. Santiago also had a lot of available open data – for example, from the census on age and income and geography, as well as open street map data.

After filtering for an appropriate sample of people who had visited multiple locations, had a known home and made at least one call a day, the researchers were able to identify 315 844 users, 51% of whom were female. They could also map the socioeconomic status of each phone user, because Chileans must provide a payslip when establishing a mobile phone contract. In combination with Chile's excellent public census data, the researchers were able to perform a stratified socio-demographic analysis. After cross-referencing this information with satellite and open street map data to determine particular points of interest, the data collaborative was able to map the exact types of trips women and men were making across the full range of socio-economic backgrounds.

The results of this innovative research found that mobility in Santiago is clearly gendered. For example, women tend to visit around 2.13 places fewer every day than men, and usually make trips to a few highly preferred locations, whereas men make more trips to a wider range of places. Notably, the research showed that women are significantly more likely to return to preferred locations than men.

Having differentiated the results by socioeconomic status, the collaborative also showed that the mobility gender gap widens as incomes decreased. Poorer women were far more bound to their local area than poorer men. However, a small gender gap remained even among the wealthiest socioeconomic band. Further analysis of socio-demographic indicators show a strong correlation between the gender gap in mobility as well as in employment. There was little difference in how unemployed and employed men used public transport, but a massive difference in the case of unemployed and employed women. A key way for policy makers to address the gender mobility gap might therefore be through policies that address this employment gap as the cause, and the mobility gap as the symptom.

Novelty

This analysis represented the first time that CDRs had been used in this detail to map the gender mobility of women. A similar study had been conducted in Seoul, but not at the same depth or with the same types of open data.

Results and impact

The research efforts undertaken for this initiative have just concluded, so it is too early to determine the extent to which it will result in changes in policy or public services. However, municipal and national government organisations have expressed interest in the findings.

Challenges and lessons learned

One particular obstacle with this completely new type of research is the cultural challenge of convincing public servants in a public sector organisation such as UNICEF of the value of the new methodology. Members of the collective from GovLab, UNICEF, ISI and the UDD all allotted significant time to convince people, particularly in the public sector and municipal and national Chilean agencies, of the importance of the new approach.

A second challenge related to translating interest in the project into action. Difficulties arose from the fact that, until the research was complete, it was difficult to prove to people that the underlying science was robust. However, Natalia Adler, then of UNICEF, mentioned to OPSI that this advocacy challenge, might better have been overcome with greater involvement from more local policy stakeholders from the start.

A key lesson learned was therefore the importance of communication – firstly, in convincing people that new methods and approaches are worth taking (traditional social scientists needed to be won over to these new methods); and, secondly, in terms of the co-operation between the teams and organisations that flowed into the data collaborative, whose structure and partnerships were key to the research.

Finally, using CDRs might raise some initial concerns about users' privacy; however, Telefónica, has a well-established process for anonymising phone numbers and user identities, which was developed to enable their private data to be shared in a transparent way for the public good. As researchers from the data collaborative noted, when you are using more detailed data, you have to do more to compensate for valid concerns about privacy.

Replicability

Santiago may have been a particularly suitable choice of a city for the project given the availability of open and private data, but researchers from the collaborative noted that it is theoretically replicable elsewhere. The methodology generated a certain set of results for Santiago, but these findings may not apply to other cities or other countries around the world. Others wishing to adapt the methodology will need to consider the extent to which if fits with their own context and operating environment.

However, the researchers did indicate that the situation has evolved substantially with the COVID-19 pandemic. As highlighted in our first Trends Report of 2020 on innovative COVID-19 solutions,[25] countries are increasingly using telecoms data to understand the mobility patterns of their population. In attempting to understand how women navigate urban spaces, the data collaborative established methodologies that have been used since and have been mainstreamed more broadly in Santiago since the pandemic began. The City of Santiago is able to use these methods to see and comprehend their citizens' needs and preferences, and through exposing its public sector researchers to these methods, better understands their potential in this crucial moment.

25 https://oe.cd/c19-innovation.

KEY THEME 02

Biometric technologies and facial recognition

Certain technologies are expanding the realm of the possible for monitoring and the use of data harvesting, and deserve more detailed investigation. Biometrics involves the use of automated tools to identify an individual through physical characteristics, such as fingerprints, iris scans or face recognition. Many people use biometrics multiple times a day, for example, by unlocking their iPhone with their fingerprint or through facial recognition. Biometrics can allow for streamlined and tailored services from government and the private sector alike. However, their usage raises a number of privacy and security concerns. Facial recognition, in particular, has been a controversial topic, as such systems can also have an inherent technological bias (e.g. when based on race or ethnic origins) (OECD, 2020b). There are also many unresolved questions about the use of biometric approaches in the present, and how they may evolve in the future.

In the 2018 Global Trends Report, OPSI and the MBRCGI explored the case of India's Aadhaar initiative,[26] the largest biometric identity programme in the world with over 1.2 billion enrolled users. Our research uncovered some of the benefits and dilemmas associated with biometric programmes, and continues to find that biometrics have largely been evaluated and used in projects on a case-by-case basis, with the technology being chosen and applied according to the needs of specific projects. However, broader ethical consideration associated with biometrics – as with any technology with the potential to be used for personal identification and surveillance – create challenges and complexities for exploring new applications. Despite the unclear terrain, governments and their partners in many areas are expanding their use of these applications. In addition, some governments and organisations are moving beyond project-by-project considerations regarding biometric applications and risks (e.g. ethics, privacy) by developing more overarching policies to guide their actions in conjunction with data regulations such as the GDPR.

Leveraging biometrics for programmes and services

The scope for biometrics has only increased since we first covered the topic, and a variety of biometric technologies have started to proliferate in differing fields. One such technology is voice biometrics. For example, the Australian Taxation Office has been steadily increasing its use of "voiceprints" (biometrics based on individual voices) to help verify the identity of service users and to ensure the security of interactions (Nott, 2018). This can improve the service experience for people, while protecting their sensitive personal details and tax information. While this usage is clearly concerned with making service delivery easier and smoother, and simultaneously increasing security for users, other usages have more complex considerations attached. For instance, in the United States, a number of prisons have been collecting and using voice prints to help ensure that prisoners are not fraudulently using the personal call quotas of other prisoners (Joseph and Nathan, 2019). However, there are concerns that this approach could be used to track who prisoners are talking to and other uses well beyond the initial remit. This has led some to think that the privacy concerns with voice prints should restrict their usage to instances when a warrant has been granted to law enforcement (Deskus and Fattal, 2019),[27] more in line with the treatment of DNA and fingerprints in many areas.

The most heated interest and debate perhaps surrounds the increasing opportunities offered by facial biometrics. AI combined with improved and extensive (and sometimes ubiquitous) camera technology and reach means that facial recognition has become accessible for a wide range of purposes. Real-world applications are already being demonstrated by governments, with significant variation in how the technology is being used and applied. For instance, facial biometrics along with other biometrics are being used for identity programmes besides the Aadhaar initiative (Box 8).

26 https://oe.cd/innovation2018.

27 www.justsecurity.org/66571/a-fourth-amendment-framework-for-voiceprint-database-searches.

Box 8: Examples of biometric identity programmes

Singapore's GovTech agency is integrating facial verification technology (see the *Facial Verification for National Digital Identity* case study later in this report) on the basis that such biometrics will by speed up login processes, thus facilitating users' ability to access government and private sector services. Implementation at the government level will also obviate the need for private companies to create their own biometric databases.

Madeira, an autonomous region of Portugal, is implementing a biometric system-on-card (BSoC) – effectively a computer the same size as a credit card – which will give users quick access to their identity metrics in order to make daily transactions. The biometrics are stored on the card itself, which Madeira believes mitigates the risk of data breaches.

These examples highlight two key issues regarding biometrics: firstly, each country's citizens, based on their cultural norms, will come to their own conclusions about the type of biometric data they are comfortable with the government using. Secondly, they highlight the importance of how data are accessed and stored. In Singapore, only profiles of users are kept (rather than actual facial images), with the data stored on a cloud database that returns a positive validation or non-validation for user authentication. Neither government employees nor private sector services using the technology for authentication ever directly access the biometric data. In India, the data are stored on many servers around the country, which is perhaps necessary given the size of the programme: – over 1 billion people are registered – but risks greater security challenges, and indeed there have been examples of compromised data. Finally, in Madeira, each user owns their own data through the BSoC.

Source: www.asianspectator.com/index.php/news/acn-business-news/4766-madeira-to-implement-groundbreaking-smart-city-technology, https://techcrunch.com/2019/01/31/aadhaar-data-leak and https://govinsider.asia/transformation/thailands-vision-for-a-self-sovereign-digital-id.

Much of biometric usage is related to policing, which can be more sensitive than other potential use cases. For instance, facial recognition has been used in a number of cities around the world to help locate suspected criminals and implement counter terrorism activities. The International Criminal Police Organization (INTERPOL) is one such entity employing facial recognition and other types of AI for law enforcement.[28] In China, facial recognition is used on transportation systems for both law enforcement and more traditional (and less controversial) fare administration (see Box 9). The emergent nature of facial recognition technology and other biometrics, more broadly, means that both the soft norms constituted by best practices, and the hard policies that shape the use and limits of the technology's application, have yet to be established in many cases. Accordingly, facial biometrics are being implemented in myriad and different ways.

Box 9: Face scanning on public transportation systems in China

The variety of applications for facial biometrics can be demonstrated by how – even within the same country and in the same field – the technology can be implemented in different ways. In China, two different examples highlight how facial recognition has been used in public transport. In the city of Zhengzhou, commuters can sign up to have their face scanned and then have their metro fare automatically deducted from their account via a pre-set payment method when boarding.

In an alternative approach, the City of Beijing is trialling facial recognition to scan and screen passengers to detect those with criminal records, as well as those known to be fare evaders, pickpockets or public nuisances.

Source: www.xinhuanet.com/english/2019-12/03/c_138602454.htm and https://asiatimes.com/2019/10/facial-recognition-easing-congestion-in-china.

28 INTERPOL and the United Nations Interregional Crime and Justice Research Institute's (UNICRI) have published Artificial Intelligence and Robotics for Law Enforcement, which explores the potential of facial recognition and other types of AI for policing, and details real-world projects already underway. See www.unicri.it/news/article/Artificial_Intelligence_Robotics_Report.

While, the uses and implications of facial recognition are still being explored, new applications of biometrics and potential risks are emerging. As noted by researchers at the AI Now Institute (Kak, 2020), advances in biometric technologies, including facial biometrics, have claimed to be able to infer demographic characteristics, emotional states and personality traits from bodily data. This progression moves beyond matching a person with a set of physical qualities, to making inferences about that person. Border control was one of the first government areas to implement facial biometrics, most commonly at airport passport gates, which match live facial scans against digital pictures stored in government databases to speed up passport control queues. New innovations are now building on the technology in this field. For instance, the European Union, through its iBorderCTRL initiative, has been exploring the potential of AI to detect micro-gestures for the purposes of "deception detection" (European Commission, 2018; Stolton, 2020). While the results are not definitive as yet, the case provides some speculative possibilities indicating avenues that governments and others may consider exploring in the future, often in combination with other types of AI analysis.

The capabilities of AI-enabled facial biometrics continue to be pushed by governments, with efforts accelerating in light of recent events. Countries have made frequent use of facial recognition to monitor and control the spread of COVID-19. In Poland, for example, the government launched a biometrics smartphone app that uses facial recognition to confirm that people infected with COVID-19 remain under quarantine, while in China facial recognition has been used to prevent citizens possibly infected with COVID-19 from travelling (OECD, 2020b). The technology has also adapted rapidly to keep up with the times. For instance, the COVID-19 crisis initially resulted in constraints on facial recognition due to mask wearing. However, significant progress has already been made in this regard (Cipriani, 2020). In the first Trends Report, *Innovative Responses to the Covid-19 Crisis*, we discussed the use of facial detection and scanning technology in Singapore to accurately analyse peoples' temperatures when wearing masks. Many governments are now exploring the use of facial recognition technology to enable "mask recognition" to ensure that people are complying with mask-related ordinances or requirements (Yan, 2020).

Facial biometric technologies are as controversial for the public sector as they are innovative, with many critics highlighting concerns about the appropriate balance between more effective services and potential bias (Box 10).

Box 10: Facial recognition privacy and bias concerns

Facial recognition technology has become a lightning rod for concerns about privacy. As the technology has matured, it has become increasingly capable of identifying faces in a crowd. By matching images from CCTV to police databases, for example, facial recognition technology can provide real-time surveillance and improve safety and security by identifying criminal suspects or missing people, among other applications. However, privacy advocates are concerned that it enables governments to gather a huge amount of information about citizens without their consent, which could be used for a number of purposes.
In addition, facial recognition technology trained on datasets which are not sufficiently diverse can reduce the accuracy of identification for some groups, leading to an increased risk of false positives. For example, police forces in the United Kingdom have come under criticism for failing to test the impact of ethnicity on prediction accuracy. An MIT study, for which the results are contested, found that multiple facial recognition tools are less accurate for black people and women, leading to potential bias on the grounds of gender and ethnicity.

There are also cases where inappropriate procedures by police forces have led to the use of poor quality input data, substantially weakening the accuracy of facial recognition software. For example, police forces in the United States have sought to match drawings of suspects, poor quality CCTV stills, computer-enhanced images and even a picture of a suspect's celebrity doppelganger to image databases. These examples suggest that clearer rules are required on precisely how the software should be used and to clarify whether a match is sufficient grounds for arrest.

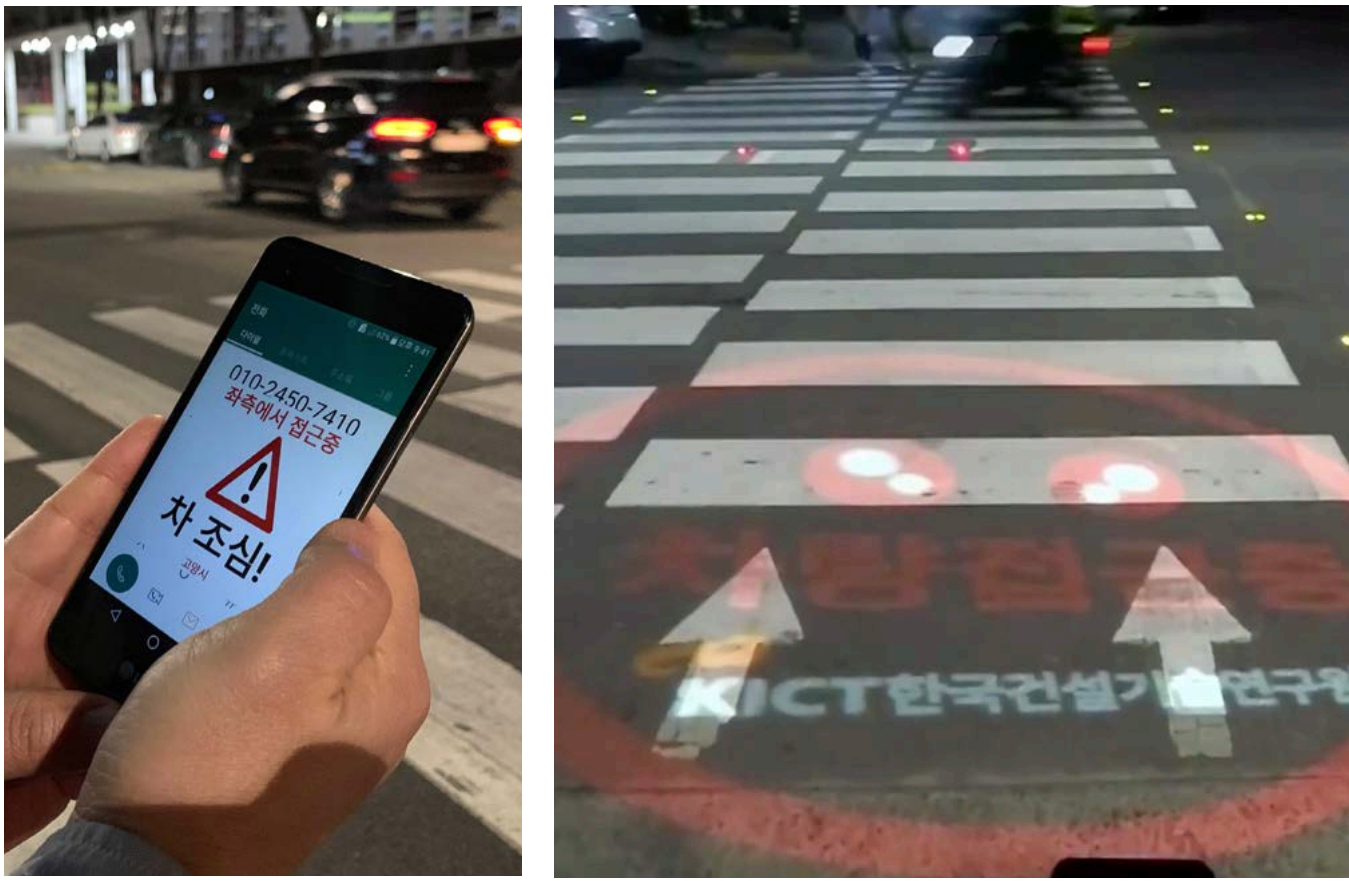
In a context of rapidly changing technology and low levels of trust in government, there are concerns that this technology gives too much power to the public sector. Contentious cases such as these are likely to spark societal debate about whether the use of facial recognition technology is consistent with respect for individual autonomy and, if so, what safeguards need to be put in place to protect liberal values. Citizens are likely to demand a proper consultation on whether the technology is being used in ways that might affect them.

Source: https://towardsdatascience.com/how-ethical-is-facial-recognition-technology-8104db2cb81b, www.bbc.co.uk/news/technology-47117299, https://medium.com/@AINowInstitute/aftera-year-of-tech-scandals-our-10-recommendations-for-ai-95b3b2c5e5, www.flawedfacedata.com; www.americaunderwatch.com and www.bbc.co.uk/news/technology-48222017.


构见能力平台
脸型比例
方形
三角脸 1%
鹅蛋脸 13%
心形脸 4%
圆形脸 80%
年龄比例
少年 14%
青年 84%
中年 2%
老年 0%
戴眼镜比例
漂亮小姐姐
福气暖男神
来宾
VIP贵宾
年龄:青年
圆形脸
不戴眼镜
戴眼镜
心情:高兴
心花怒放，喜事不断神采飞扬
心情:平静
鹅蛋脸
方形脸
机遇一鸣惊人

Other biometrics are also being explored aside from face, fingerprints and voice. For instance, in China, facial recognition has been complemented by "gait analysis", which identifies people by the way they walk.[29] In the United States, the Department of Defense has developed a laser that can identify people from a distance by their heartbeat.[30] Moving away from identification of individuals, a milder example that could be classified more as body *detection* rather than body *recognition* is being deployed in Korea with a focus on public safety. In Ilsan, it became apparent to policy makers that there was a growing relationship between the high rate of smartphone usage and the extremely high rate of traffic accidents involving pedestrians. People were crossing the street while looking at their phones, rather than paying attention to oncoming traffic. Local media termed these people "smartphone zombies", or "smombies". To address this issue, the Korea Institute of Civil Engineering and Building Technology (KICT) has designed an intervention that uses a medley of lights, lasers and phone alerts to alert smombies when they approach a crossing, and to encourage them to look up from their phones and more safely navigate road crossings (Figure 4).

Figure 4: Smartphone zombie phone alerts and street warnings



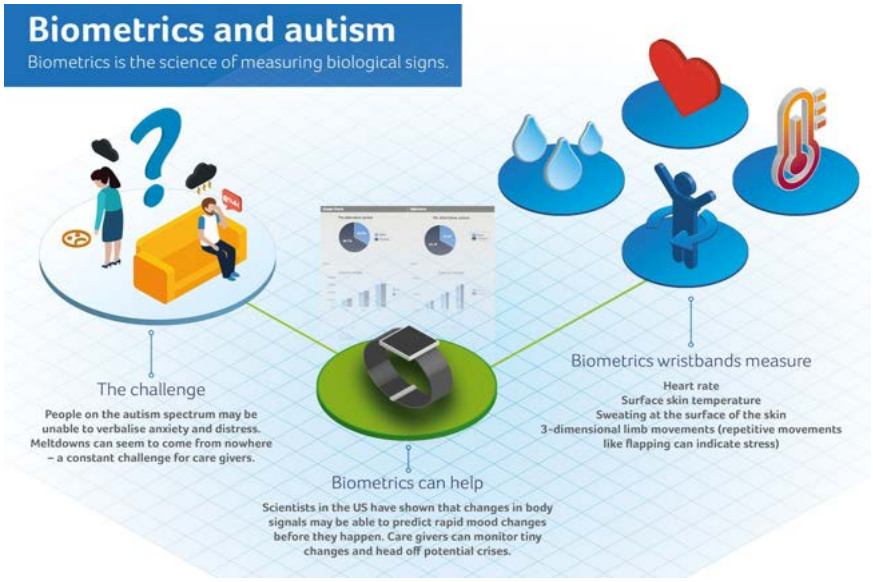
Source: www.reuters.com/article/us-southkorea-smartphones-crossing-idUSKCN1R0029.

Healthcare is also a field in which biometric data has potential. One particularly innovative example comes from the Wirral, in Liverpool. The autism charity, Autism Together, working in conjunction with the local council, has designed an innovative programme to test the potential for using biometrics to transform the care of those with severe autism. The charity, which operates as a service provider, with the support of the council as well as funding from the National Health Service, designed a wearable biometric wristband to be worn by people with autism to monitor periods of high anxiety. The wristband detects though biological changes in surface skin temperature, heart rate and perspiration. This innovation was particularly suitable for some individuals with autism who may be non-verbal or unable to communicate how they feel. As such, this biometric data could provide unique insights into their feelings and emotions, and allow for the provision of better care.

29 www.privacy-ticker.com/chinese-police-uses-gait-recognition-for-identification.

30 www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat.

Figure 5: How Autism Together's biometrics tool may aid treatment of people with autism



Source: www.autismtogether.co.uk/biometrics-could-be-a-game-changer-in-autism-care.

Governments at local, national and even international levels will undoubtedly continue to explore biometric technologies to improve the efficiency, effectiveness and responses of public policies and services. Accordingly, governments and other organisations are designing frameworks and principles to help guide others as they explore this complex field. Some relevant examples include the Biometrics Institute's Ethical Principles for Biometrics (Box 11), and the Safe Face Pledge, which focuses on facial biometrics (Box 12).

Box 11: Ethical Principles for Biometrics

The Biometrics Institute is an international association representing a multi-stakeholder community consisting of government agencies, companies, civil society and academia. Its mission is to promote the ethical use of biometrics and biometric analysis, and, to this end, the institute elaborated the "Ethical Principles for Biometrics" which uphold seven key principles:

1. **Ethical behaviour.** Members must act ethically even beyond the requirements of law. Ethical behaviour means avoiding actions which harm people and their environment.
2. **Ownership of biometrics and respect for individuals' personal data.** Individuals have significant but not complete ownership of their personal data, especially their biometrics, requiring their personal data, even when shared, to be respected and treated with the utmost care.
3. **Serving humans.** Technology should serve humans and should take into account the public good, community safety and the net benefits to individuals.4. Work with collaborators and partners to improve privacy and security practices, based on ongoing evaluation and refinement.
4. **Justice and accountability.** We accept the principles of openness, independent oversight, accountability and the right of appeal and appropriate redress.
5. **Promotion of privacy enhancing technology.** We promote the highest quality of appropriate technology use including accuracy, error detection and repair, robust systems and quality control.
6. **Recognising dignity and equal rights.** We support recognition of dignity and equal rights for all individuals and families as the foundation of freedom, justice and peace in the world, in line with the United Nations Universal Declaration of Human Rights, must be supported.
7. **Equality.** We promote planning and implementation of technology to prevent discrimination or systemic bias based on religion, age, gender, race, sexuality or other descriptors of humans.

In expanding on this work, the organisation launched the "first comprehensive, universal privacy guidelines for biometrics" in 2019.

Source: www.biometricsinstitute.org/wp-content/uploads/Biometrics-Institute-Ethical-Principles-Final_1019.pdf, www.biometricsinstitute.org/privacyguidelines.

Box 12: The Safe Face Pledge

The Safe Face Pledge is a joint project of the Algorithmic Justice League and the Center on Privacy & Technology at Georgetown Law in Washington, DC. It serves as a means for organisations to make public commitments towards mitigating the abuse of facial analysis technology. It includes four primary commitments:

- **S**how Value for Human Life, Dignity and Rights
  - Do not contribute to applications that risk human life
  - Do not facilitate secret and discriminatory government surveillance
  - Mitigate law enforcement abuse
  - Ensure your rules are being followed
- **A**ddress Harmful Bias
  - Implement internal bias evaluation processes and support independent evaluation
  - Submit models on the market for benchmark evaluation where available
- **F**acilitate Transparency
  - Increase public awareness of facial analysis technology use
  - Enable external analysis of facial analysis technology on the market
- **E**mbed Commitments into Business Practices
  - Modify legal documents to reflect value for human life, dignity and rights
  - Engage with stakeholders
  - Provide details of Safe Face Pledge implementation

Source: www.safefacepledge.org/press-release.

Designing policies for managing biometric technologies and data

Polls seeking to understand whether people know how governments use their personal data show that a significant proportion have no knowledge of what their governments do with such information, including biometrics data (see Figure 6). This may have serious consequences. For example, when new uses emerge for such technologies, people who remain uninformed may come to conclusions based on false or incomplete information, resulting in public perceptions of services that may shape their attitudes and consent. Another risk is that governments may be tempted to implement technologies that might not garner public approval, if people fully understood their implications. Beyond the issue of lack of public understanding, governments must also grapple with the complex ethical and privacy issues that using such technology creates. Demand for more ethical practices has been increasing, reflecting a widespread interest in ensuring that data, including biometrics, are used in ways that respect the public interest and deliver trustworthy outcomes.

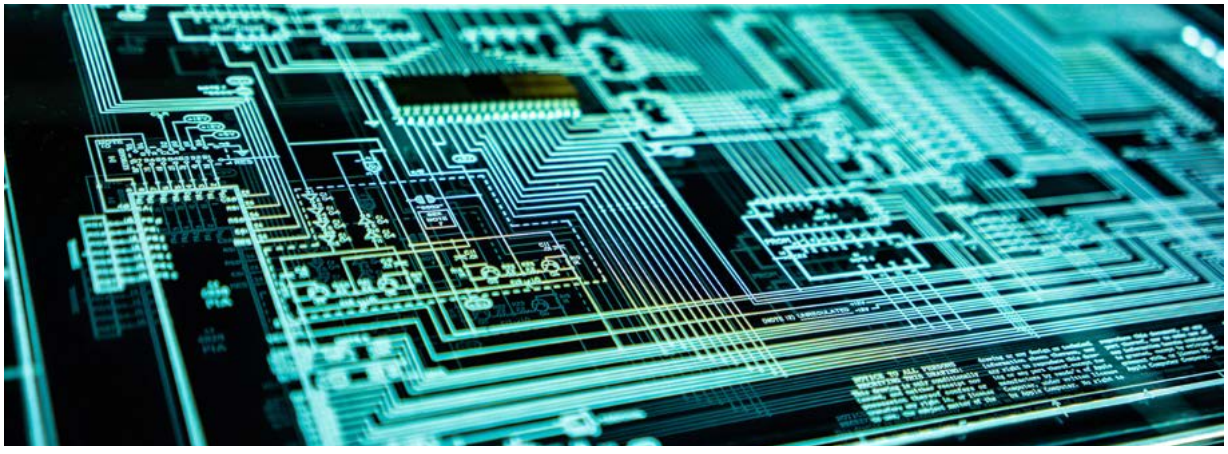
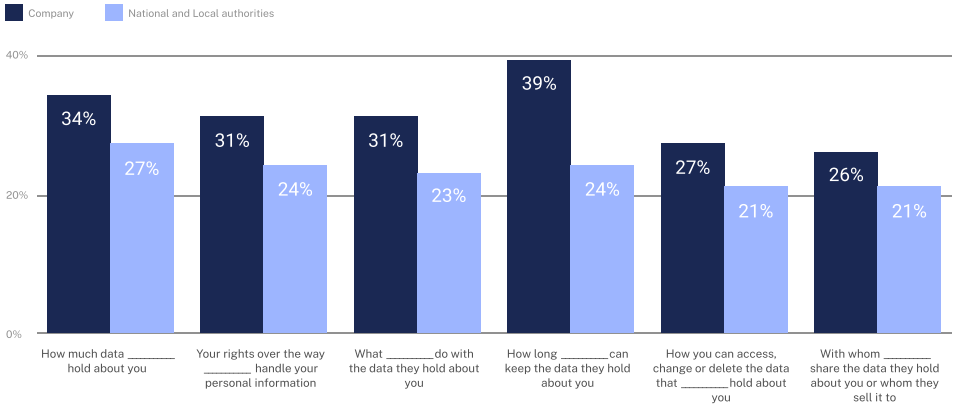


Figure 6: Most citizens do not know how government uses their personal data



Source: Ipsos-World Economic Forum poll (www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf).

In terms of biometric data, governments have generally considered the surrounding issues on a project-by-project basis. However, as the possibilities of these technologies become more tangible, some governments and other organisations are working to put in place broader guidance and ground rules to assure citizens of their appropriate and trustworthy usage and controls, thereby implementing consistency in decision making for biometric initiatives, at least to some extent. As biometrics is fundamentally an issue of data use, some data regulations describe arrangements for how the use of biometric technology might be interpreted, most notably the EU's General Data Protection Regulation (GDPR) (Box 13). While project-by-project checks against such data rules can be sufficient, broader biometric policies can add additional requirements and/or tackle additional considerations to help ensure more standard usage of biometrics.

Box 13: GDPR and biometrics

The European Union's 2017 General Data Protection Regulations (GDPR) refers to biometric data as a "special category of personal data" or "sensitive data", which "merit higher protection", because they offer particular risks to the individuals' fundamental rights and freedoms were they to be used in the wrong way.

Therefore, while biometric data are protected under the same regulations as other forms of data through the GDPR, they also have their own provisions as a special category of data. The GDPR includes the following (non-exhaustive, but relevant to biometric data) requirements:

- Consent must be "freely given" for the data to be shared or processed in any unintended ways.
- An assessment must be undertaken of the data risks to the persons whose data are being used.
- Data processors must offer full transparency about data are being used and allow data subjects to access and delete their stored personal data.
- Proportionality between data use and information security must be ensured.

In general, the GDPR states that biometric data can be used if proportionality is maintained between the use and the information security risks, and if the right specific measures are in place to protect the rights and freedoms of the person and their data. It also states that there are limited instances of public interest, such as healthcare-related crisis, where biometric data can be used without the consent of the person – although such data can never be processed for other purposes if collected for that purpose.

Source: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data and www.oecd.org/gov/digital-government/the-path-to-becoming-a-data-driven-public-sector-059814a7-en.htm

In response to some of these difficult questions, the cities of Portland, Oregon and San Francisco, California, recently announced strict bans prohibiting city agencies from using facial recognition technology and barring businesses from using it in public areas within city limits (Ellis, 2020; Conger, Fausset and Kovaleski, 2019). The bans were introduced with the intent of protecting privacy, with the San Francisco ban already in effect and the Portland prohibition due to take effect at the start of 2021.

Perhaps the most straightforward policy for ensuring privacy and security related to biometric data are protected is San Francisco and Portland's blanket "no". However, the public's attitudes towards the use of this technology and the tensions involved differ – and failing to explore the potential of certain biometrics may lead to missed opportunities and potential for real improvements to services, as well as individuals who are less informed about the pros, cons and technicalities of biometric solutions. Research indicates that many people are open to the idea; for example, Pew Research polling (Smith, 2019) has indicated that most American citizens (56%) actually trust law enforcement and government to use facial recognition responsibly, despite the anecdotal perception that the United States, which places great weight on personal liberties and freedoms, might have a population opposed to facial recognition. This polling also highlights how attitudes differ massively across demographic groups, implying that different communities likely hold different perceptions of the technology. Other research (Riley et al, 2009; Janssen and van den Hoven, 2015) demonstrates that cultural norms influence popular views on privacy, which data and approaches are ethical to use, and what restrictions or permissions should be required. Generating a stable consensus across society regarding the various trade-offs between privacy, transparency and service quality, will therefore be challenging. However, governments should actively seek to understand how their citizens feel about the technology, to ensure that any related projects and policies reflect the views of the people, and that the right services are subsequently designed.

For example, a different approach is that taken by Oregon's neighbour, the State of Washington. In a new law,[31] also coming into effect in 2021, the government has made explicit the permitted uses, expectations and safeguards for the introduction or use of facial recognition by agencies. Microsoft, a significant industry player, hailed in particular the introduction of explicit testing requirements, transparency and accountability measures, and the protection of civil liberties as enshrined in the legislation.[32] Microsoft is not the only company pushing for reforms in how facial biometrics are used, with IBM making waves in June 2020 when it announced[33] that it was exiting the business of facial recognition entirely, calling for a "national dialogue on whether and how facial recognition should be used by domestic law enforcement". Other states such as Illinois and Texas have also developed privacy laws, but no federal law has yet been passed on the use of biometric data in the United States (OECD, 2018).

On the other side of the Atlantic, the European Commission has recognised in its Artificial Intelligence White Paper[34] that "the gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights". Under the General Data Protection Scheme, processing of biometric data for the purpose of uniquely identifying a person is limited to a set number of grounds, in particular whether there is substantial public interest. Given this, "AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards". Perhaps reflecting the understanding that citizen expectations and perceptions for the use of this technology can vary greatly, the European Commission undertook a consultation to consider what these safeguards should be, with 28% of respondents apparently supporting a ban on the use of biometric remote identification in publicly accessible places.[35] The Commission considered but did not pass a five-year moratorium on the use of facial recognition in public places (Espinoza, 2020).

Another problem facing governments designing any public policy in this area is the issue of "function creep". Function creep in the area of biometrics and other surveillance technologies and data can be described as the process whereby the functions of a particular data type or technology expand beyond the original intent as consented to by individuals (Mordini, 2009). As established, most people are not fully aware of the ways in which governments use their data, but different groups still hold varying opinions on how they should be used. Therefore, logically, consent for a particular use of biometric technology or data is a very narrow thing. Governments should not assume that citizens and residents will consent to a different use of the same technology in five years' time – or even potentially the same use once the implications become clearer. This was exactly the conclusion reached by the International Committee of the Red Cross (ICRC) when designing their own biometric policy (see Designing a Biometric Policy for Humanitarian Aid case study), as their policy commits them to periodically re-examining what their users and beneficiaries want and accept from their use of the technology (ICRC, 2019).

31 http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf.

32 https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation.

33 www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms.

34 https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

35 www.euractiv.com/section/data-protection/news/commission-will-not-exclude-potential-ban-on-facial-recognition-technology.

Indeed, OPSI and the MBRCGI's research identified consent as the final issue – though certainly not the final consideration in dealing with biometric technologies – that constrains or complicates the development of new policies for this emergent technology.[36] The National Digital Identity case study for Singapore (see the next section of this report) constructed their service around the key principle of consent. In fact, as Singapore has focused on developing the digital literacy of the population,[37] and the government's national identity programme SingPass has been running since 2003,[38] it may be easier to establish in this instance that the citizens were able to give informed consent to using the service. A yet-unpublished survey from Singapore's GovTech agency indicates that 75% of citizens are willing to use facial verification as part of the scheme. However, many populations will not be equally informed about government usage of their biometric data. And, in other situations, the power dynamics may encourage some people to offer consent for a service because they desperately need its benefits, even if they might be uncomfortable with how their data are being stored or accessed or shared. Singapore addresses this by ensuring that biometrics constitute just one non-mandatory option among multiple means to access the same services.

The ICRC, however, did not design a policy around consent due to their perception of the artificiality of consent in humanitarian crises, where beneficiaries might consent to things they do not understand or to which they would not otherwise consent due to their desperate need. Instead, they used the alternate legal infrastructure around their organisational mandate to interpret when the balance between the public benefit of using this type of data and the risks to the beneficiaries of the aid merits use of the technology (Hayes and Marelli, 2020). As such, while consent is often framed as fundamental for the ethical use of biometric data – for example in the GDPR – a holistic understanding of the uses and possible impacts of the technology may reveal situations where alternate frameworks are needed to design a policy that ensures the technology is used in an appropriate and ethical way.

The wealth of difficult ethical debates, heterogeneous cultural feelings towards the technology across demographic groups, and the lack of general expertise on the part of average citizens all represent challenges to how governments consider and use biometric technologies – and also constitute possible reasons why few international sets of guidelines exist for how this technology should be used. Nonetheless, the technology is being used, and for now, governments often continue to judge on a case-by-case basis the relative merits and strengths of these technologies against the potential misuses or risks relating to the absence of suitable safeguards to ensure their proper and proportionate use.

In order to seize the potential of these technologies while mitigating risks and ensuring ethical approaches, government may want to consider developing focused guidance on the use of biometrics and the data behind them, in a manner consistent with existing data rules, and incorporate the viewpoints and opinions of their citizens and residents in a way that allows these topics to be continuously revisited and reconsidered. Over time, these efforts could contribute to coherent policy frameworks and shared social norms to govern the use of these technologies. The OECD's "Good Practice Principles for Data Ethics in the Public Sector" (see Box 5 earlier in this report) may help governments as they think through considerations on a project-by-project, or seek to build out more targeted biometrics policy initiatives. Boxes 6, 7, 11, and 12, also presented earlier in this report, can help provide additional provide additional prompts for consideration and provide further guidance on approaches these issues.

36 www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometrics-questions.

37 www.moe.gov.sg/microsites/cos2020/refreshing-our-curriculum/strengthen-digital-literacy.html.

38 www.singpass.gov.sg/singpass/common/aboutus.

KEY THEME 02: Case Study

Facial Verification for National Digital Identity

Singapore

As biometric identification technology proliferates, some governments are exploring how they can best use this technology to enhance the lives of their citizens. Singapore is incorporating facial verification technology to allow citizens to access services both in government and private business as part of their National Digital Identity (NDI) programme. To this end, Singapore's GovTech agency is building on the existing *SingPass* digital identity card platform, which allows users to access hundreds of digital government and private sector services, to allow users to access these services and more through facial verification technology. The verification procedure checks the face of a citizen in real time against a digital face associated with their account, all remotely via cloud servers, ensuring that consent remains fundamental to the process. The aim of the project is to allow Singapore residents and businesses to make even more convenient and secure transactions, and thereby facilitate the growth of a digital economy.[39]

39 Unless otherwise indicated, the information for this case study was sourced from an interview with Quek Sin Kwok, Senior Director of the National Digital Identity Platform and Products in the Government Technology Agency of Singapore (GovTech).

The problem

As biometric technologies continue to grow and evolve, governments and businesses on the leading edge are looking to realise the potential of technology such as facial verification to make identification processes more efficient. Many of us use facial verification in our day-to-day lives to unlock our mobile phones or to use automatic gates at border controls. However, as the technology grows in use, so will the number of databases containing facial biometric data, thus increasing the risk of a bad faith actor obtaining access to the data, as well as incompatibility and potentially unnecessary duplicated labour between facial verification systems. Without central co-ordination, the ultimate risk is that every private company and government agency will create their own biometric database (Horizon State, 2018).

Government-issued ID cards are now well established in many countries around the world, and allow residents to access a wealth of services. In countries such as Singapore, ecosystems are being built around ID cards, which require authentication to use these services. The *SingPass* platform has been operational since 2003, and through it citizens can access government services, including those related to taxes and welfare, as well as private sector services, through the use of a single ID centralised under the government. Since 2017, Singapore has integrated this platform into a National Digital Identity (NDI) project (see Box 14), which hopes to create digital identities for each citizen to enable them to connect more easily with wider range of services both inside and outside government.

Box 14: Singapore's National Digital Identity programme

The National Digital Identity (NDI) programme, launched in 2017 by the Singaporean Prime Minister, is regarded as a "strategic national project". Part of its ambition is to reduce dependency on physical identity cards and eliminate them altogether by 2025, replacing them with a variety of digital verification mechanisms. Currently, around 4 million out of 6.5 million residents use *Singpass*, Singapore's NDI platform. Half of these also use *Singpass Mobile*, the mobile phone application. The NDI has three key purposes:

1. To digitally empower residents, by facilitating faster, safer and more reliable transactions between citizens, businesses and government agencies.
2. To digitally connect businesses so that they are able to author digital services with trust and take advantage of new technologies transforming the way that they do business.
3. To drive the digitisation of the wider economy, by allowing more trusted flows of data across organisations, sectors, the country and even internationally.

Source: Interview with GovTech officials.

NDI programmes can enable the provision of services at vast scales, but they have also faced a number of challenges, however, especially when they incorporate biometrics. For example, India's Aadhaar project, which was featured in the 2017 Global Trends Report, has registered over 1.2 billion Indians and has collected their fingerprints and iris scans. It is by far the largest NDI and biometric verification scheme in the world with 1.2 billion Indians' fingerprints, photos and iris scans captured, which has enabled tens of billions of financial transactions, and facilitated related benefits such as doubling the amount of women with bank accounts.[40] However, it has experienced a number of issues too: some reports indicate that problems with its integration into food subsidy programmes have resulted in difficulties with accessing food (Biswas, 2018; Frayer and Khan, 2018). There have also been data security breaches, with one security failure offering public access to details of over 166 000 workers (Whittaker, 2019). Any NDI programme using biometrics will have to contend with issues such as these.

SingPass has also had its own distinct challenges. It typically uses a 2-factor authentication system for digital transactions,[41] with user ID and password being one of the factors. One of the biggest challenges facing *SingPass*, according to its operators, is the use of passwords, which present a number of issues. These include users forgetting their password at the verification point, requiring them to undergo a lengthy reset process which takes up time and resources. Furthermore, passwords can be shared between people, allowing someone else to access one's account. Other access factors, such as sending codes

40 See https://oe.cd/innovation2018.

41 www.smartnation.gov.sg/what-is-smart-nation/initiatives/Strategic-National-Projects/national-digital-identity-ndi.

by text message to phones, also have security vulnerabilities. Another solution, the use of a physical token, can be impractical as citizens have to adapt their behaviour to carry them – and they can still be lost, forgotten or even stolen. It was therefore clear to Singapore that their NDI project should explore additional factors of verification.

An innovative solution

As a result of these identified issues with authentication, Singapore's NDI project is seeking to use biometric data to streamline the authentication process for citizens when using *SingPass*, Singapore's NDI platform. The fundamental objective of the NDI project, which is overseen by Singapore's Government Technology Agency (GovTech), is to digitally empower people and businesses in Singapore, by making verification and identification processes faster, simpler for users, and more reliable and secure. GovTech determined that the integration of biometric verification would facilitate faster and more secure transactions between people and services, and would, accordingly, complement the digital infrastructure Singapore is building out to grow its digital economy and government.

While different methods will always suit different needs, GovTech recognised that facial verification technology (see Box 15) may be the most suitable biometric to integrate into *SingPass*. This was for three reasons. First, the government already had a database of faces at its disposal from passport photographs, which it could mobilise – with the consent of users – for this new purpose. Second, facial verification technology did not require the creation and distribution of new bespoke technology. These reasons are consistent with GovTech's fundamental principle of leveraging existing data and technology. Conversely, fingerprints or voice recognition would require the government to create a new system to collect, store and analyse this data, and, if fingerprints were used, it would require the creation and distribution of fingerprint scanners. In addition, people are already used to facial verification, which was the third factor in making it the most suitable biometric solution. For instance, individuals are accustomed to unlocking their smartphones with their faces, and the use of the technology at automatic gates in airports is now common around the world.

Box 15: Facial verification versus facial recognition

GovTech officials see facial verification as different from facial recognition both in terms of usage and who benefits from the process. They see facial verification as checks to whether the user is the person they claim to be at specific moments for specific purposes. Facial recognition, on the other hand, refers to technology that scans groups of people in an indiscriminate manner to identify particular individuals. Facial verification technology empowers the user by allowing them to be authenticated against an image they have taken themselves. Individuals identified through facial recognition have not consented to having their image taken, and the process is used to benefit those performing the scan rather than the person being scanned.

How does the facial verification behind *SingPass* work? Citizens create an account and then consent to the integration of facial biometric data from their passport photo into their *SingPass* profile. Once their face is linked to their *SingPass*, residents are able to use their camera-equipped computer or mobile device to scan their face in order to access options such as digital government services and private sector services, such as banking. In physical locations, facial scanners scan the faces of residents. The facial scans are then sent digitally to GovTech's secure cloud servers where they are compared to pseudonymised facial profiles. The server then sends an accuracy score to the service provider for the comparison between the two images, and the user is verified to proceed. Service providers that use the facial verification system as a form of identity authentication never see the data that the government has on file, only a score indicating the closeness of the scan to these data (McDonald, 2020).

Figure 7: A user has their face scanned as part of the *SingPass* verification process

Source: GovTech Singapore.

GovTech have paid careful attention to a number of concerns that have been raised about biometrics. First of all, they ensure that the data they control is protected through a number of security measures, such as strong encryption and strict access controls. They also ensure that service providers (government agencies, companies) never see a picture that the user scans or the data saved on record. Any image sent to the cloud is deleted after a month. Furthermore, the image against which the photo is compared is not the original raw passport photo, but rather a "template" image built out of key points of the facial attributes of the original image. This means that even the select few with strict access to the data will never see the actual faces of people. On top of this, the database is situated in a single location on the cloud, secured with the latest digital security measures. This model is different to that of Aadhar, which operates on a federated model with multiple copies of the database. Singapore officials believe that having a single well-protected source reduces the chances of access by bad-faith actors.

In addition, GovTech have ensured that citizen consent is at the heart of their design. Citizens will never be obliged to use facial verification for any service – there will always be an alternative option. Facial verification is simply one factor that a user can choose (or not) to combine with other factor(s) for multi-factor verification. In addition, all uses by service providers must be purpose-driven – when a provider wants to use the service, they must apply and describe the purpose. GovTech only approves an application if the purpose is for the clear benefit of individuals, and will not permit uses of the service that go beyond the declared and approved purpose. This should prevent "function creep" whereby facial verification proliferates into other services until citizens are obliged to use it or be unable to access new services. For any one service, the citizen has to actively consent (or revoke consent) to the use of facial verification in the specific situation, which, crucially, does not commit them to its future use in any other situation. It was key to GovTech that consent was incorporated as fundamental design principle. This helped generate trust in the system by citizens and increase the likelihood of uptake.

To date, the facial verification software has been trialled in a number of consumer-facing public agencies, such as kiosks at Singapore's tax office, the Inland Revenue Authority of Singapore (IRAS) and the Public Service Centre of Our Tampines Hub – an integrated community and lifestyle destination. It is also being used in a branch of the bank DBS, and citizens can now also use the technology through computers at home to open an online bank account using their face as ID. Facial verification also is planned for security purposes in ports – a fundamental infrastructure in Singapore – as well as for exams to ensure that students sit their own test (many countries such as Singapore have problems with public exam fraud) (McDonald, 2020). To facilitate roll-out, GovTech is creating software development kits and plug-ins for companies who wish to participate in this programme. As such there is no need for companies to invest in designing individual software; rather, they can transition seamlessly to the biometric verification system proposed by GovTech. Such ecosystem-building activities can support adoption and are recognised by the OECD's Digital Government Policy Framework (OECD, 2020c)[42] as an important indicator of digital maturity.

Going forward, Singapore will evaluate how to expand the programme both in terms of services that can be accessed through facial verification, as well as the extent to which other biometrics (e.g. fingerprints) can be incorporated. The ambition is for NDI to proliferate throughout government and the private sector in Singapore. As well as being used more broadly inside Singapore, there is potential for the system to grow internationally. Firstly, it is hoped that non-Singaporean businesses accessing Singaporean markets will be able to use the system, as well as Singaporean citizens abroad, who may be unable to receive SMS verification texts due to different telecom networks.

Novelty

Singapore's use of facial verification represents the first time that a government has attempted to mobilise this type of facial biometric technology as proof of identity for services at this scale, with the previous main utility of the technology being passport verification at borders. In addition, the ambition of the programme and its ability to be leveraged by the private sector for user authentication has the potential to be fully integrated into the broader economy in new ways.

Results and impact

The NDI's biometric verification is planned for roll-out over a three-year period, starting in 2020. However, trials in public and private sector environments have offered proof of concept. Feedback from the services in which it has been incorporated indicate that the verification process is working exactly as planned. Facial verification has significantly reduced queueing times in government agencies where it has been implemented with user kiosks. Furthermore, implementation has also reduced queues for lines to re-set passwords.

User perspective

GovTech made certain that the technology works for users, as empowering citizens was part of the ambition of facial verification. It conducted a study (GovTech Singapore, forthcoming) to assess the comfort of citizens with government use of biometrics in their services, the outcome of which demonstrates cultural acceptance of the technology. Early analysis of the results indicated that 70% of respondents are comfortable with facial recognition technology and 75% are willing to use facial recognition technology.

Challenges and lessons learned

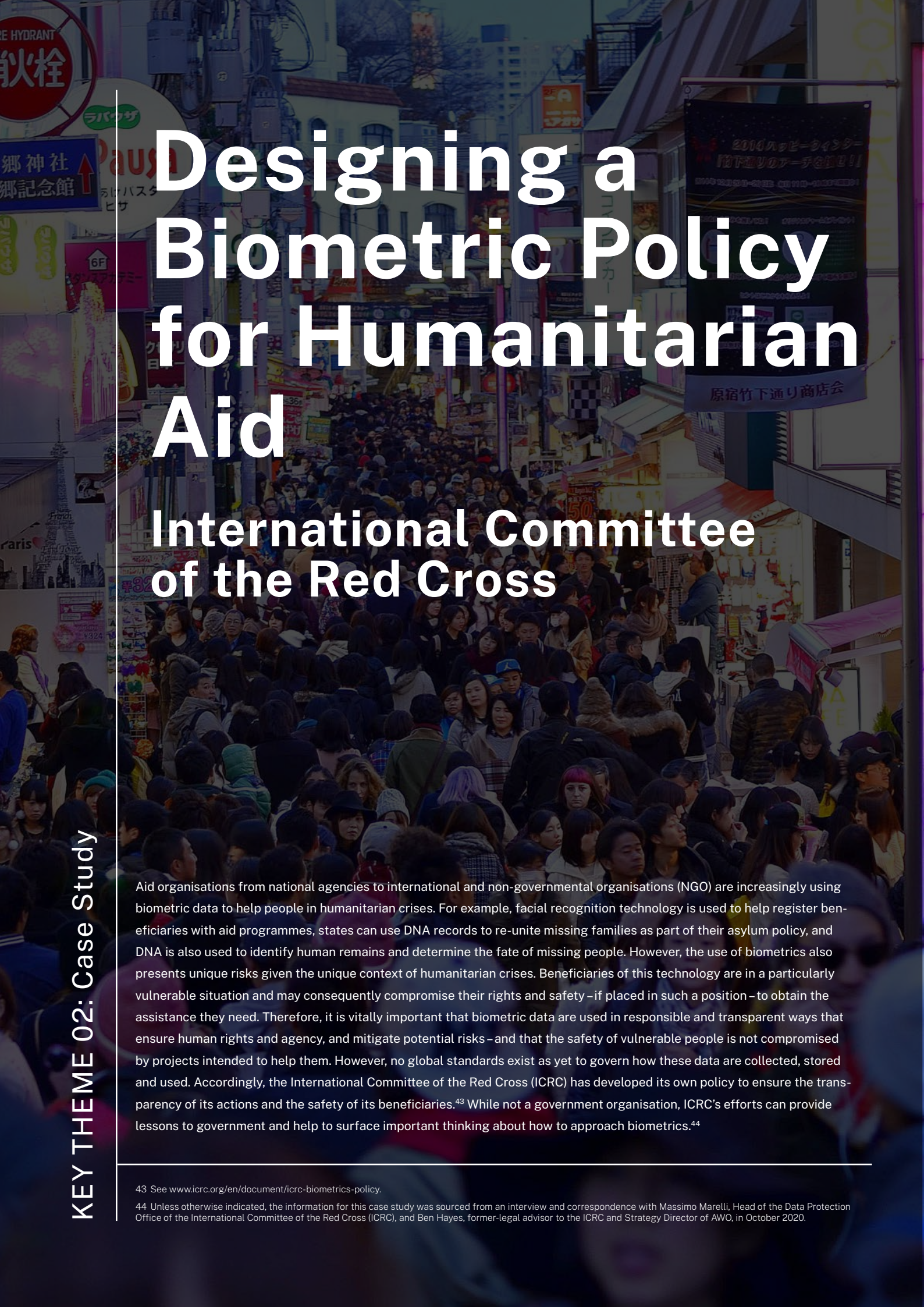
Singapore as a system is particularly suitable for big digitisation innovations in the public sector. Firstly, there is broad cultural acceptance of identification technology, as indicated by the GovTech survey and by the broad uptake of SingPass among users. Secondly, Singapore and GovTech are able to move quickly with innovative projects due to what Kwok Quek Sin, the Senior Director of GovTech, describes as "simpler, flatter" layers of government (Lago, 2019), as well as strong support from political stakeholders. Singapore's openness to both the technology and having a centralised government platform that serves to authenticate and identify citizens were also important factors. Finally, Singapore's development has always operated according to three principles: being open, connected and trusted. By building out their project with these principles in mind, they have ensured that consent is at the heart of the design, and have worked to create a system that is trusted by citizens.

42 https://oe.cd/il/diggovframework.

Replicability

As touched on earlier, GovTech is interested in international collaboration to expand the service it has developed. To promote replication of Singapore's approach, GovTech is open to sharing its technology with other governments to aid with replication, once it's been further tested and has matured. Replicability of the technology is further facilitated by the manner of storage on the cloud. GovTech has identified three speculative ways in which broader international collaboration could happen around this technology:

1. Bilateral agreements between countries where each agrees to recognise the other's systems based on trust and equivalence of legal standards and technology.
2. A global organisation establishing a set of standards that could harmonise the activities of every country.
3. A distributed system in which checks for verification are carried out by multiple sources rather than just one.



KEY THEME 02: Case Study

Designing a Biometric Policy for Humanitarian Aid

International Committee of the Red Cross

Aid organisations from national agencies to international and non-governmental organisations (NGO) are increasingly using biometric data to help people in humanitarian crises. For example, facial recognition technology is used to help register beneficiaries with aid programmes, states can use DNA records to re-unite missing families as part of their asylum policy, and DNA is also used to identify human remains and determine the fate of missing people. However, the use of biometrics also presents unique risks given the unique context of humanitarian crises. Beneficiaries of this technology are in a particularly vulnerable situation and may consequently compromise their rights and safety – if placed in such a position – to obtain the assistance they need. Therefore, it is vitally important that biometric data are used in responsible and transparent ways that ensure human rights and agency, and mitigate potential risks – and that the safety of vulnerable people is not compromised by projects intended to help them. However, no global standards exist as yet to govern how these data are collected, stored and used. Accordingly, the International Committee of the Red Cross (ICRC) has developed its own policy to ensure the transparency of its actions and the safety of its beneficiaries.[43] While not a government organisation, ICRC's efforts can provide lessons to government and help to surface important thinking about how to approach biometrics.[44]

43 See www.icrc.org/en/document/icrc-biometrics-policy.

44 Unless otherwise indicated, the information for this case study was sourced from an interview and correspondence with Massimo Marelli, Head of the Data Protection Office of the International Committee of the Red Cross (ICRC), and Ben Hayes, former-legal advisor to the ICRC and Strategy Director of AWO, in October 2020.

The problem

Biometrics are already used widely in refugee and humanitarian operations; however, different organisations use this technology in different ways given their legal mandates and objectives. For example, the International Committee of the Red Cross (ICRC) exists to provide humanitarian assistance to people in need. The organisation does not have an explicit legal mandate to use biometrics, due to its status as an international organisation whose mandate is derived from international humanitarian law, namely the Geneva Conventions of 1949 and their Additional Protocols and Statutes that pertain to the ICRC.[45] Accordingly, it currently applies its own data protection framework, the "ICRC Rules on Personal Data Protection"[46] to interpret how to use biometric laws, in conjunction with an analysis of the technology and associated risks, to decide how to use data on a case-by-case basis (see Box 16).

Box 16: How the ICRC uses and might use biometrics

Prior to the adoption of its biometrics policy, the ICRC employed the technology in limited ways, in cases where specific objectives may not have been achievable without its use. These included:

- The restoration of family links by using DNA comparisons to confirm links between relatives.
- Adding fingerprints to travel documents issued by the organisation (but not to a database) for those who need to travel internationally but lack ID documents.
- Forensics, such as examining and identifying human remains.

ICRC staff have also started to conceive of potential ways that biometrics might further enhance their work, including:

- The use of facial recognition to identify missing people from their database of photos of missing and sought persons.
- To manage aid distribution, through a distributed token-based system and never via a central database, by simplifying and speeding up processes on the ground, thus limiting the exposure of ICRC staff to potentially dangerous situations.

Source: Interview with Massimo Marelli, Head of the ICRC's Data Protection Office, and Ben Hayes, legal advisor to the ICRC and Director at AWO. https://ainowinstitute.org/regulatingbiometrics-hayes-marelli.pdf
https://blogs.icrc.org/inspired/2019/09/06/humanitarian-artificial-intelligence

The approach to use of biometrics differs across the humanitarian aid sector. For example, the United Nations High Commissioner for Refugees (UNHCR) – the UN agency principally responsible for refugees – has 7.2 million biometric records on file and has used them to conduct 60 million operations (UNHCR, 2019). The UNHCR does have a specific mandate to identify refugees and asylum seekers and to provide them with identity documents; and, as such, is able to justify the use of biometrics such as fingerprint records because they can help track, locate, monitor or identify dislocated people according to different needs (Hayes and Marelli, 2020). The heterogeneous legal mandates of different organisations have therefore led to different uses of the technology within the sector, and have perhaps limited the opportunity to develop a shared regulatory framework regarding the technology.

As explored in the discussion in the chapter, biometrics are already being used in this area, but their use raises a number of challenges. One key problem relates to data security, as refugees and those requiring humanitarian assistance are by their nature a vulnerable cohort. Many refugees are fleeing regimes or conflicts in which people are actively seeking to do them harm. Such people might want to access any data gathered on the refugees. Accordingly, the safety and security of biometric systems in humanitarian situations is particularly acute. A second problem revolves around the issue of consent in such situations. Vulnerable people requiring the assistance of aid organisations, whether governments or non-governmental organisations, experience a particular power dynamic with aid responders, whereby they may be more likely to accept conditions that they would otherwise not accept in exchange for help, such as submitting to biometric collections and pro

45 See https://app.icrc.org/discover-icrc/2-what-is-the-icrc.html.

46 See https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection.

grammes (Burt, 2019). Therefore, if the beneficiary of aid thinks that they can only receive assistance if they consent to sharing data, then it is unlikely that consent will be "freely given" – a key consideration in data protection law, which would legally invalidate such consent. Additionally, many refugees lack a significant amount of formal education, and may not understand the full risks and consequences of such programmes and their implications, limiting consent to a superficial commitment. Finally, there is the risk of "function creep", whereby biometric databases are gradually used for services other than that for which they were originally intended. This situation is particular problematic because the beneficiaries of humanitarian aid are often difficult to reach, making consent for any new uses more difficult to obtain (Burt, 2019).

Given the heterogeneous organisational mandates for use of this technology, and the varying uses to which it has been put and the mix of issues in play, few explicit policies exist to determine how it may be used for humanitarian aid. As a result, aid organisations, as well as other organisations and governments more broadly, tend to decide how to apply the technology on a case-by-case, project-by-project basis, using existing conventions that regulate the use of personal data. For example, some non-governmental organisations and EU states, which operate under GPDR, as described in Chapter 2, use biometric data under its "special category of personal data" because it places the data subject at particular risk. Its collection is permitted "only where necessary to achieve … purposes for the benefit of natural persons and society as a whole", including "the management of health and social care services and systems". On the other hand, the ICRC, with its distinct legal status, which is closer to an international organisation, does not directly fall under GDPR, but rather has its own data protection regulations. Given this unique legal status, and their growing use of the technology, they sought to establish a more cohesive guiding force behind their current and future biometrics efforts.

An innovative solution

Given the growing use of biometrics in the field and within the organisation itself, as well as the issues such usage raises and the lack of explicit guidance, the ICRC to create its own specific biometric policy. The process started by examining current uses of the technology within the organisation and their existing Data Protection Policy. They also examined the various ways in which the ICRC was already using biometrics, in order to understand the varying internal interpretations of existing regulations and determine how a unified policy would affect existing projects. The team conducting this work also spoke with existing programmes about the potential future uses of biometric data, as an essential first step in identifying proportionality considerations regarding the balance between privacy and utility. Following this deliberative process, the ICRC Assembly adopted the ICRC Biometrics Policy in August 2019, establishing the roles and responsibilities for the use of how legitimate use of this technology. Box 17 lists some of the practices allowed under the adopted policy.

Box 17: Key features of the Biometric Policy

- The continued usage of fingerprints on travel documents issued by the ICRC In limited situations for persons who have no valid identity papers.
- The use of biometric identification for security systems restricting access to confidential information and/or mission-critical resources such as servers and control rooms on ICRC premises.
- The use of biometrics including fingerprints, facial scans and DNA to identify human remains.
- The use of facial biometrics to analyse digitised photos to trace separated or missing people.
- The use of biometric data to ascertain the identity or fate of specific individuals relating to abductions or attacks on ICRC staff.
- The collection of biological reference samples for DNA testing to assist family reunifications (on a case-by-case basis).
- The use of biometrics to provide beneficiaries with token-based verification credentials, such as a card to verify their identity upon receipt of aid, in place of other identification mechanisms.

Source: www.biometricupdate.com/201906/unhcr-reaches-7-2m-biometric-records-but-critics-express-concern and www.icrc.org/en/document/icrc-biometrics-policy.

Particular attention has been paid to the issue of consent. As discussed in Chapter 2, GDPR privileges consent as a vital component in authorising the sharing of personal information between organisations. Indeed, the ICRC's Personal Data Protection Policy requires informed consent from beneficiaries for their data to be used, stored and shared. However, during interviews with OPSI, ICRC staff said that consent for biometric purposes in humanitarian emergencies would be somewhat artificial, due to the desperation of those seeking treatment or services, and a lack of in-depth knowledge about the implications of their agreement. The ICRC therefore had to develop an additional policy framework – the Biometrics Policy – to ensure that a balance is struck between using of the data for good while mitigating consequences that compromise the privacy and security of beneficiaries. This balance involves ensuring that any use is "in the public interest" – an important element in the ICRC's Rules on Personal Data Protection (and also found in other frameworks such as the GDPR) – and understood via its humanitarian mandate in the Geneva Conventions and statues for the ICRC. It can also use biometrics if there is a "legitimate interest" away from mandate-related activity, such as protecting a server or control room.

One debate that arose during development of the policy concerned the usage of biometrics in the distribution of aid. As explained above, some staff argued for the use of biometrics to streamline the process of aid distribution on the ground, potentially saving time and improving safety for ICRC staff. However, the ICRC Data Protection Office determined that this usage was not explicitly justified by their Rules on Personal Data Protection, but conceded its potential utility, if it could be designed in a way that did not compromise the rights of the people. As a result, a compromise was reached – a token-based system whereby beneficiaries may be issued physical tokens containing their biometric data. This solution ensures that the aid beneficiaries retain control of their data and are never added to a biometric database, thus reducing the chances of their biometric information being compromised.

The ICRC is also constrained in terms of the types of biometric data it may process. In accordance with their legal mandate and the public interest, the following different technologies are permitted at specific moments:

- Fingerprinting using ink and biometric scanners for the purposes of identifying remains
- Fingerprinting using biometric scanners to enrol staff and beneficiaries into biometric verification systems
- Facial recognition for the purpose of matching facial images to find missing persons
- Comparison of DNA profiles to find matching relatives.

The ICRC has worked hard to ensure that its policy is as transparent and open as possible, uses the minimum data necessary and stores only that which is needed. For example, fingerprints for travel documents still use ink prints rather than a biometric equivalent; biometrics cannot be used for routine security controls; and family reunion cases can only employ DNA profiling when so allowed by a specific regulation. Similarly, the policy establishes a number of responsibilities for the ICRC. For example, the organisation must explain to the aid beneficiaries why they are using the data, including data-sharing arrangements, regardless of the basis for the processing. The ICRC is also restricted from sharing the biometric data with third parties – including governments.

Finally, another key element of the Biometrics Policy is ongoing and continuous evaluation. The need for biometrics and the associated challenges are very real, but are also constantly evolving, as may the technology itself. As a result, the ICRC is committed to constantly evaluating and re-evaluating their project, talking to academics and technology experts to ensure that their policy is constantly up-to-date and reflects contemporaneous usage, and strikes an ethical balance that is appropriate for the ICRC given the organisation's remit.

Novelty

Biometrics are an emerging issue but one that is of particular importance for refugee operations, due to the associated risks. Policies exist that partially govern elements of biometric data (e.g. EU's GDPR), but most organisations and governments lack a policy specifically governing the use, storage and protection of biometric data in humanitarian aid situations. As such, the novelty of the case derives from the ICRC's internal process of establishing their own biometric policy – one that explicitly explores possible usages and balances them with the ethical concerns of this emergent technology.

Results and impact

Perhaps the most significant benefit for the ICRC is that the process – and the resulting policy – has allowed the organisation to reflect on its current and future usage of biometric technology. Existing projects are now able to understand how their usage fits with an explicit policy, and to proceed with greater confidence. By providing a clear policy framework, the ICRC has also accelerated the development of future biometric projects. Programme managers can now refer to a single policy document that clearly defines the limits and parameters of the technology, rather than evaluating multiple legal frameworks that govern its use.

Challenges and lessons learned

The ICRC's previous experiences were key in shaping the policy, along with consultations with stakeholders; however, they also represented a challenge, as a new policy could have forced the ICRC to change certain existing practices. Resolving certain issues within the policy also required "innovative compromises", such as the token-based solution, which emerged as a result of dialogues with stakeholders within the organisation who genuinely wanted and needed a policy. Friction caused by existing problems during the policy design process ultimately provided moments of clarity and allowed for the establishment of mutual understanding.

Other useful lessons learned included the importance of timing the intervention correctly. If certain aspects are left too late, then norms will have already formed and essentially unwritten policies will have been developed by default, rather than by design. Policy makers would be led by existing practices and may struggle to shape the way forward. While this is not insurmountable, it does signal the need to explore these issues early. The ICRC also learned that it is important to incorporate people into the design process to ensure buy-in. Not everyone will agree with the conclusions, but if a policy is co-developed and based on common assumptions, and includes a willingness to compromise when necessary, people will be more accepting of the final outcome.

Replicability

This case study provides a useful framework for how governments might develop their own policies regarding the use of biometric data, as well as insights into the sorts of problems with which they will have to contend. For example, governments might be well served by adopting a similar process: considering current and potential future usage, and evaluating existing legal frameworks, in order to understand the contemporary and future impacts of the policy. The important issue of consent, which was heavily discussed by the ICRC during the elaboration of the Biometric Policy, may also prove a point of discussion for future governments, in order to balance how consent can be given and understood, and to establish the extent of "public interest use".

There may also be potential in scaling up such approaches to an international framework. This may prove challenging, though, given how governments already use biometrics in different ways in different policy areas, and have different cultural norms on this topic. It may be worth exploring the feasibility and potential of an international approach, however, given the increasing proliferation of the technology.


CONVENZIONE DI GINEVRA 12 AGOSTO 1949

Recommendations

New technologies allowing for the collection and application of new types of data and observations about people are proliferating, and governments around the world are exploring how they might engage with them. The case studies collected by OPSI and MBRCGI indicate great potential to empower the public if governments apply these emergent technologies in a transparent and adept fashion, with the trust of their people. However, as with any emergent technologies, governments must experiment with possible approaches, and carefully examine and explore relevant considerations. The full implication of these technologies will only become clear over time and with testing, and concerns regarding misuse and the potential for compromising the privacy and data of citizens and residents are legitimate.

The use of data harvesting, monitoring, surveillance and biometrics for application such as facial recognition involve highly complex issues that need to balance multiple concerns and respect the core values and expectations of government. The case studies included here underline the need for care, and to work with people to build trust and gain informed consent when applying these technologies. The following recommendations are offered as a guide for countries as they engage with these issues:

1. **Actively engage with the issues raised by these technologies.** These emergent technologies offer significant perceived value to the wider economy and will likely become a fixture of our multi-jurisdictional world. Accordingly, governments need to take an active role in deciding how these technologies are used by developing regulatory frameworks that ensure the technology is not misused and, instead provide the demonstrated benefits to citizens while limiting unwanted effects. This cannot be done without first-hand knowledge and experience. Moreover, different organisations or countries may reach different conclusions, based on their different historical, social and cultural settings and approaches. Therefore, it is vital that governments engage openly with any concerns raised by their citizens and residents, in order to reach a mutual understanding about how this technology should and should not be used. If governments procrastinate, the norms regarding how we use the technologies may be shaped by other organisations and actors – rightly or wrongly – that do not necessarily represent the best interests of citizens.

2. **Prioritise earning trust from the public in order to successfully implement services that leverage these technologies.** Trust is vital to ensuring that citizens accept and use the technology, and is rooted in the knowledge that the information collected about them is used in appropriate and commonly accepted ways. Without trust, citizens will be reticent to use new technologies proposed by their government. At a minimum, the OECD recom mends that citizens understand what data are being collected about them (OECD, 2019), how these data are being used, how they are stored and for what duration. In practice, the use of the technologies must also correspond to citizens' expectations. Governments must apply the technologies in ways that citizens accept and want, but remain cognisant that this can change over time, sometimes very rapidly. For this reason, governments must take an active role in engaging with the issues raised by the technologies, and allow public debate to generate understanding which can be built upon. The very best efforts will go further, actively generating trust by embedding and communi cating principles such as openness and transparency into their very functioning. When citizens use services that they know have been designed in this manner, their trust in government should increase.

3. **Work collaboratively across national borders in order to understand the limits, pitfalls and opportunities of these technologies.** Many of these technologies, or at least the power to leverage them, will not remain within national borders. The data generated by the use of mobile applications and the burgeoning Internet of Things, and the ability to recognise individuals and ascertain personal information about them, are hard to quarantine to one country.[47] Expectations about what is and is not allowed will also be shaped by different country experiences, and the results will be compared. Governments could consider how to collaborate in both exploring but also constrain ing the use of such technologies.

47 For example, see www.politico.eu/article/ex-uk-cyber-chief-warns-on-chinese-data-grab/amp.

Conclusion

Governments have increasing amounts of data about their citizens and the world at their fingertips, and have a responsibility to use these data and information actively to improve the lives of people, as the COVID-19 crisis has demonstrated. As the first OPSI and MBCRGI report of 2020 on *Innovative Responses to COVID-19* indicated, new technologies are being used in innumerable ways to understand the movement of people, track with whom they interact, and even measure biometric information about their bodies to improve the overall health of citizens. These methods are saving lives and are widely accepted, highlighting a broad understanding that governments can indeed find a balance between using these new methods to improve the lives of their citizens while managing legitimate concerns around issues such as privacy and security.

This report demonstrates that these activities are just one aspect of an emerging trend where governments use data and information about their citizens in new and innovative ways. Novel methods are allowing new types of data to be collected on scales and speeds previously unseen. Real-time data collection can also help inform emergency response services, and allow governments to make more informed policy decisions.

Questions, however, loom over the use of this sort of technology, in particular around privacy and security. What if this information was used in the wrong way, or by the wrong people? Trust has therefore emerged as a core issue. The public must understand how their data are being collected, stored and used. However, there remains a large gap in the technical

literacy of populations concerning the possibilities of this technology. Accordingly, openness and transparency is incredibly important – governments must actively demonstrate that they are using these technologies in the interest of citizens, in order to generate and retain their trust.

These debates around biometrics have played out, for example, in the realm of facial recognition. The Singapore and ICRC case studies in this report show that the technology itself does not necessarily pose a problem, as long as governments abide by the correct principles and have the right safeguards in place. If the right governance and infrastructures exist around data security, the appropriate technology is selected for the right reasons, and commitments are made to be transparent and open about its use, then people are willing to accept different technologies in different situations.

Currently, these issues are arising and being addressed on a case-by-case basis. Too few countries or organisations have engaged in public debates about the use of these technologies in order to generate policy frameworks, which, if properly implemented, would constrain negative consequences, while enabling growth, through the added confidence and faith of people and businesses. If governments are going to get to grips with this technology – and they must, for the sake of their citizens – then it must necessarily be accompanied by the development of frameworks around the world governing its application.

References

Alvarez Vilanova, J. (2018), "A data-led approach to tackling homelessness: 7 lessons from Luton Council", *Policy in Practice*, http://policyinpractice.co.uk/a-data-led-approach-to-preventing-homelessness-7-lessons-from-luton-council.

BBC News (2020, 17 September), "California and Oregon 2020 wildfires in maps, graphics and image", www.bbc.com/news/world-us-canada-54180049.

Biswas, S. (2018, 27 March), "Aadhaar: Is India's biometric ID scheme hurting the poor?", *BBC News*, www.bbc.com/news/world-asia-india-43207964.

Brown, D., G. McGranahan and D. Dodman (2014), *Urban Informality and Building a More Inclusive, Resilient and Green Economy*, IIED, London.

Burt, C. (2019, 24 June), "UNHCR reaches 7.2M biometric records but critics express concern", *Biometric News*, www.biometricupdate.com/201906/unhcr-reaches-7-2m-biometric-records-but-critics-express-concern.

Cipriani, J. (2020, 15 September), "How to unlock the iPhone faster when wearing a face mask if your phone lacks Touch ID", *cnet*, www.cnet.com/how-to/how-to-unlock-the-iphone-faster-when-wearing-a-face-mask-if-your-phone-lacks-touch-id.

Conger, K., R. Fausset and S.F. Kovaleski (2019, 14 May), "San Francisco bans facial recognition technology", *The New York Times*, www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

Del Real, J.A. (2019, 24 June), "Can 'big data' help fight big fires? Firefighters are betting on it", *The New York Times*, www.nytimes.com/2019/06/24/us/wildfires-big-data-california.html.

Deskus, C. and J.R. Fattal (2019, 17 October), "A Fourth Amendment framework for voiceprint database searches", *Just Security*, www.justsecurity.org/66571/a-fourth-amendment-framework-for-voiceprint-database-searches.

Ellis, R. (2020, 10 September), "Portland passes nation's toughest restriction on facial recognition technology", *OPB*, www.opb.org/article/2020/09/09/portland-passes-nations-toughest-restriction-on-facial-recognition-technology.

Espinoza, J. (2020, 12 February), "EU backs away from call for blanket ban on facial recognition tech", *The Financial Times*, www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5.

European Commission (2018), "Smart lie-detection system to tighten EU's busy borders", Brussels, https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726.

Feldstein, S. (2009), *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, Washington, DC, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

Frayer, L. and F.L. Khan (2018, 1 October), "India's biometric ID system has led to starvation for some poor, advocates say", *NPR*, www.npr.org/2018/10/01/652513097/indias-biometric-id-system-has-led-to-starvation-for-some-poor-advocates-say?t=1602171416923.

Gauvin, L. et al. (2020), "Gender gaps in urban mobility", Humanities and Social Sciences Communications, Vol. 7/11, https://doi.org/10.1057/s41599-020-0500-x.

Givetash, L. (2020, 28 July), "Australian wildfires declared among the 'worst wildlife disasters in modern history'", *NBC News*, www.nbcnews.com/news/world/australian-wildfires-declared-among-worst-wildlife-disasters-modern-history-n1235071.

GovTech Singapore (forthcoming), Study.

Hayes, B. and M. Marelli (2020), *Reflecting on the International Committee of the Red Cross's Biometric Policy: Minimizing Centralized Databases*, AI Now Institute, New York, https://ainowinstitute.org/regulatingbiometrics-hayes-marelli.pdf.
Horizon State (2018, 19 September), "How governments can let citizens call the shots", *GovInsider*, https://govinsider.asia/connected-gov/how-governments-can-let-citizens-call-the-shots.

ICRC (2019, 16 October), "The ICRC biometrics policy", *International Committee of the Red Cross* (website), www.icrc.org/en/document/icrc-biometrics-policy.

Janssen, M. and J. van den Hoven (2015), "Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?", *Government Information Quarterly*, Vol. 32/4, pp. 363-368, https://doi.org/10.1016/j.giq.2015.11.007.

Joseph, G. and D. Nathan (2019, 30 January), "Prisons across the U.S. are quietly building databases of incarcerated people's voice prints", *The Intercept*, https://theintercept.com/2019/01/30/prison-voice-prints-databases-securus.

Kak, A. ed. (2020), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, New York, https://ainowinstitute.org/regulatingbiometrics.pdf.

Lago, C. (2019, 16 August), "Inside Singapore's National Digital Identity programme", *CIO*, www.cio.com/article/3432144/inside-singapore-s-national-digital-identity-programme.html.

Loukaitou-Sideris, A. (2014), "Fear and safety in transit environments from the women's perspective", *Security Journal*, Vol. 27, pp. 242-256, https://doi.org/10.1057/sj.2014.9.

Lyon, D. (2007), *Surveillance Studies: An Overview*, Polity Press, Cambridge, UK, www.wiley.com/en-ca/Surveillance+Studies%3A+An+Overview-p-9780745635927.

McDonald, T. (2020, 25 September), "Singapore in world first for facial verification", *BBC News*, www.bbc.com/news/business-54266602#:~:text=Singapore%20will%20be%20the%20first,to%20the%20country's%20digital%20economy.

Mordini, E. (2009), "Ethics and policy of biometrics", in M. Tistarelli, S.Z. Li and R. Chellappa (eds), *Handbook of Remote Biometrics. Advances in Pattern Recognition*, Springer, London, https://doi.org/10.1007/978-1-84882-385-3_12.

Nott, G. (2018, 15 February), "The ATO now holds the voiceprints of one in seven Australians", *Computerworld*, www.computerworld.com/article/3474235/the-ato-now-holds-the-voiceprints-of-one-in-seven-australians.html.

OCED (2020a), *Building Capacity for Evidence-Informed Policy-Making: Lessons from Country Experiences*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/86331250-en.

OECD (2020b, 23 April), "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics", *OECD Policy Responses to Coronavirus (COVID-19)*, www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636.

OECD (2020c), "The OECD Digital Government Policy Framework: Six dimensions of a Digital Government", *OECD Public Governance Policy Papers*, No. 02, OECD Publishing, Paris, https://doi.org/10.1787/f64fed2a-en.

OECD (2019a), *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/059814a7-en.

OECD (2019b), "OECD Open, Useful and Re-usable data (OURdata) Index: 2019", *OECD Policy Papers on Public Governance* No. 1, OECD Publishing, Paris, www.oecd.org/gov/digital-government/policy-paper-ourdata-index-2019.htm.

OECD (2018), "New technologies and 21st century children: Recent trends and outcomes", OECD *Education Working Paper* No. 179, OECD Publishing, Paris, https://one.oecd.org/document/EDU/WKP(2018)15/en/pdf.

OECD (2017), *Fostering Innovation in the Public Sector*, OECD Publishing, Paris, https://doi.org/10.1787/9789264270879-en.

Riley, C et al. (2009), "Culture & biometrics: Regional differences in the perception of biometric authentication technologies", *AI & Society*, Vol. 24, pp. 295-306, https://doi.org/10.1007/s00146-009-0218-1.

Smith, A (2019, 5 September), "More than half of U.S. Adults trust law enforcement to use facial recognition responsibly", *Pew Research Center*, www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly.

Stolton, S. (2020, 6 April), "MEP: Public has a 'right to know' about Commission's lie detector tech", *Euractiv*, www.euractiv.com/section/digital/news/mep-public-has-a-right-to-know-about-commissions-lie-detector-tech.

UNHCR (2019, 19 June), "Introductory Remarks of Andrew Harper, Director of the Division of Programme Support & Management", Global Strategic Priorities (EC/70/SC/CRP.1 3), 75th Meeting of the Standing Committee, United Nations High Commissioner for Refugees, Geneva, www.unhcr.org/excom/standcom/5d0b43537/75th-meeting-standing-committee-presentation-director-division-programme.html.

Yan, W. (2020, 11 September), "Face-mask recognition has arrived – for better or worse", *National Geographic*, www.nationalgeographic.com/science/2020/09/face-mask-recognition-has-arrived-for-coronavirus-better-or-worse-cvd.

Whittaker, Z. (2019, 1 February), "Indian state government leaks thousands of Aadhaar numbers", *TechCrunch*, https://techcrunch.com/2019/01/31/aadhaar-data-leak/?guccounter=1.

Witze, A. (2020, 10 September), "The Arctic is burning like never before – and that's bad news for climate change", *Nature*, www.nature.com/articles/d41586-020-02568-y.

Yu, M., C. Yang and Y. Li (2018), "Big data in natural disaster management: A review", *geosciences*, Vol. 8/165, www.mdpi.com/2076-3263/8/5/165/pdf-vor.

OECD
BETTER POLICIES FOR BETTER LIVES

OPSI Observatory of Public Sector Innovation

مركز محمد بن راشد للابتكار الحكومي
MOHAMMED BIN RASHID CENTRE FOR GOVERNMENT INNOVATION

WORLD GOVERNMENT SUMMIT

trends.oecd-opsi.org