

# Data Sharing in Disruptive Technologies: Lessons from Adoption of Autonomous Systems in Singapore

Si Ying Tan<sup>a</sup>, Araz Taeihagh<sup>b</sup>  and Devyani Pande<sup>b</sup>

<sup>a</sup>Leadership Institute for Global Health Transformation, Saw Swee Hock School of Public Health, National University of Singapore, Singapore, Singapore; <sup>b</sup>Policy Systems Group, Lee Kuan Yew School of Public Policy, National University of Singapore, Singapore, Singapore

## ABSTRACT



Autonomous systems have been a key segment of disruptive technologies for which data are constantly collected, processed, and shared to enable their operations. The internet of things facilitates the storage and transmission of data and data sharing is vital to power their development. However, privacy, cybersecurity, and trust issues have ramifications that form distinct and unforeseen barriers to sharing data. This paper identifies six types of barriers to data sharing (technical, motivational, economic, political, legal, and ethical), examines strategies to overcome these barriers in different autonomous systems, and proposes recommendations to address them. We traced the steps the Singapore government has taken through regulations and frameworks for autonomous systems to overcome barriers to data sharing. The results suggest specific strategies for autonomous systems as well as generic strategies that apply to a broader set of disruptive technologies. To address technical barriers, data sharing within regulatory sandboxes should be promoted. Promoting public-private collaborations will help in overcoming motivational barriers. Resources and analytical capacity must be ramped up to overcome economic barriers. Advancing comprehensive data sharing guidelines and discretionary privacy laws will help overcome political and legal barriers. Further, enforcement of ethical analysis is necessary for overcoming ethical barriers in data sharing. Insights gained from this study will have implications for other jurisdictions keen to maximize data sharing to increase the potential of disruptive technologies such as autonomous systems in solving urban problems.

## ARTICLE HISTORY

Received 6 September 2022  
Accepted 9 November 2022

## KEYWORDS

Data sharing; autonomous systems; disruptive technologies; Singapore

**CONTACT** Araz Taeihagh  [spparaz@nus.edu.sg](mailto:spparaz@nus.edu.sg), [araz.taeihagh@new.oxon.org](mailto:araz.taeihagh@new.oxon.org)  Lee Kuan Yew School of Public Policy, National University of Singapore, 469C Bukit Timah Road, Li Ka Shing Building, Level 2, #02-10, Singapore, 259772, Singapore

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

## 1. Introduction

According to the United Nations, 55 per cent of the world's population lives in urban cities, and this figure will increase to 68 per cent by 2050 (United Nations 2018). The use of disruptive technologies in smart city developments can help solve challenges related to increased urban density with limited resources by increasing the efficiency of service provision (Radu 2020; Tan and Taelhagh 2020). Smart cities have digitally enabled the construction of critical infrastructures capable of providing intelligent services in industries such as transport, healthcare, environment, entertainment, and energy (Falco 2020; Zhang et al. 2017). Internet of Things (IoT), big data, blockchain, artificial intelligence, data analytics, machine learning and cognitive learning are examples of new technologies used in smart cities (Radu 2020). These technologies are used in autonomous systems in sectors such as agriculture, defence, transportation, health, space exploration, and manufacturing.

Autonomous systems refer to a range of powered physical systems that possess cognitive abilities to self-direct themselves; they are aware of their surrounding environment, context and tasks allocated to them, operate without human intervention, and generate outcomes in uncertain or known conditions (Pande & Taelhagh (forthcoming)). The range of autonomous systems comprises autonomous vehicles (AVs) (also known as driverless cars), manufacturing systems, artificial companions, smart homes, autonomous weapons, unmanned underwater vehicles, and unmanned air vehicles (McCarthy 2009; Watson and Scheidt 2005). AVs have been one of the most prominent autonomous systems, with ongoing trials being undertaken in Singapore, San Francisco, Las Vegas, Detroit, Palo Alto, Pittsburgh, San Jose (Hawkins 2019), London (Ridden 2019), cities in France, Dubbo (Australia) (Frost 2019), Shanghai and Changsha (Central China) and others. Autonomous systems are beneficial for saving time and effort, reducing labor costs, quick decision-making and can be used in hostile places where human presence is not feasible (Leikas, Koivisto, and Gotcheva 2019; Spichkova and Simic 2015). However, using AVs has implications for privacy, cybersecurity, ethics, and algorithmic bias in smart cities (Lim and Taelhagh 2018, Lim & Taelhagh 2019). Similarly, the use of autonomous systems in long-term care was found to have these concerns along with ethical issues such as compromising personal autonomy and social interactions, as well as objectification and infantilisation of users (Tan & Taelhagh 2021).

Smart cities generate and consume complex data and are advancing the trend of data sharing (Russo and Feng 2020). A key concern in the use of autonomous systems in smart city development is data management and data sharing, as there are ramifications for privacy, cybersecurity, and transparency. While data governance has been identified as a key challenge for governments by OECD, data sharing is deemed important to promote technological innovation and advance smart city development. To address the potential conflict between data governance and data sharing, an internationally agreed set of rules—OECD Recommendation on Enhancing Access to and Sharing of Data—has been framed as guidelines for governments (OECD 2021b).

Autonomous systems are a key segment in deployment of disruptive technologies in smart city developments. Against this backdrop, we formulate the following research question: What are the effective strategies for public and private agencies to

overcome the different types of barriers to data sharing in adopting autonomous systems in smart cities? To answer this research question, we examine the development of data sharing initiatives and various strategies deployed to promote the adoption of autonomous systems in Singapore. Singapore is a suitable case as data sharing is touted to generate social and economic benefits worth 1 to 2.5 per cent of the GDP of Singapore (PricewaterhouseCoopers 2021), and Singapore is the forerunner in the smart city development and adoption of disruptive technologies, particularly in the area of testing and deploying autonomous systems (Smart Nation and Digital Government Office 2022, KPMG International 2020). Anchoring on these insights, we propose recommendations for overcoming data-sharing challenges deemed relevant to policymakers and practitioners.

This paper is structured in 5 sections. [Section 2](#) discusses the framework on barriers to data sharing and highlights the development of data sharing initiatives and regulations pertaining to adopting autonomous systems in Singapore while [Section 3](#) explains the strategies used to overcome the barriers to data sharing in autonomous systems in Singapore. [Section 4](#) discusses the lessons for governing data sharing that can be applied to other jurisdictions and [Section 5](#) concludes and proposes agendas for future research.

## 2. Background

### 2.1. Barriers to data sharing for autonomous systems

The IoT is a key tool for disruptive technologies used in smart cities. When these technologies are connected, they generate data consistently and pass it through the internet using IoT (Abu-Elkheir, Hayajneh, and Ali 2013). In AVs, data from the installed sensors are interpreted, and decisions are made about the vehicle's operation and adjustment to the changing environment (Lim & Taeihagh 2018). Privacy and ethics regarding data storage start in the process of IoT when a query leads to data generation, collection, aggregation, and delivery to units within IoT, as well as pre-processing, processing and analysis of the stored data (Abu-Elkheir, Hayajneh, and Ali 2013; Pande & Taeihagh (forthcoming)). This is evident in the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications in AVs (Lim & Taeihagh 2018) and communication within robots (Wang et al. 2015). In addition, the quality of the data and data labeling in such systems is also a concern (Liang et al. 2022).

Trust and security concerns arise with the requirements of an open and standardized infrastructure (Uckelmann, Harrison, and Michahelles 2011). The environment for IoT for data sharing must be trustworthy to prevent sabotage or cyber-attacks that would impact the tasks of robots (Ray 2016). In addition, procedures are required to be put in place to protect the integrity, trust, and confidentiality of data to ensure that no malicious codes are running for a task being done by a robot (ibid.). With this arises the significance of privacy that data sharing can infringe upon. Privacy can be understood as confidentiality to prevent the unauthorized sharing of information of users (Nissenbaum 2004). The threat to the privacy of individuals is evident in autonomous systems like personal care robots that can record

conversations and take pictures which could lead to information leakage. Collecting the vast amount of data and processing them enables autonomous systems to discover patterns, but that could infringe on the privacy of individuals by identifying their characteristics (Raso et al. 2018; Such 2017). Unmanned drones that monitor crowds impact the privacy of individuals as well as groups, and information transmission via V2V and V2I communication in AVs reveal vehicle movement that are risks to the privacy of individuals (Finn, Wright, and Friedewald 2013; Glancy 2012).

With the use of IoT, the risk of privacy and cybersecurity are evident. These risks could result in different barriers to data sharing in developing novel technologies in smart cities. Adapting a framework on barriers to data sharing by Van Panhuis et al. (2014), we find that the key categories for barriers to data sharing within technologies encompass technical, motivational, economic, political, legal, and ethical (explained in Table 1).

## 2.2. Methods: data curation

The data used to analyze Singapore's strategies in overcoming barriers to data sharing in autonomous systems adoption were curated from the discussion notes and transcripts of 45 interviews with different stakeholders conducted between 2018 to 2020, coupled with the collection of secondary data sources including journal articles, policy documents, technical reports, policy briefs and media releases on autonomous systems implementation in Singapore. The interviews targeted policymakers and bureaucrats in the transport, healthcare and technology sectors, private developers of autonomous systems, academics, data scientists and healthcare workers. Questions pertaining to the implementation processes of different autonomous systems in the transport and healthcare industries were posed during the interviews, and sections of data related to data sharing access and barriers were extracted whenever these issues were discussed during the interviews. We identified secondary data sources such as

**Table 1.** Barriers to data sharing for autonomous systems (adapted from Van Panhuis et al. (2014)).

Categories of barriers to data sharing	Explanation
Technical barriers	These barriers arise due to the lack of capacity to make data available or use it, not being able to preserve it, language barriers, constraints due to data formats, and lack of standards.
Motivational barriers	These are barriers to data sharing due to institutional or personal beliefs that lead to no incentive to share data, the higher opportunity cost of data collection, criticism for data providers, and disagreement among data providers.
Economic barriers	These barriers are caused due to economic damage when data is released and a lack of technical resources to share data.
Political barriers	These refer to the lack of trust between users and providers, regulations restricting data sharing, and no standards or guidelines for data sharing.
Legal barriers	They comprise legal instruments such as data ownership, copyright protection, and privacy protection that limit data sharing.
Ethical barriers	These arise due to normative principles involving deliberations on the benefits of data sharing and not being able to ensure fairness in data sharing when data providers do not get due credit.

government reports, announcements, and Singapore standards and guidelines for specific autonomous systems between 2016 and 2022 to fill any subsequent information gaps. We categorized these data based on different categories of barriers to data sharing identified by Van Panhuis et al. (2014), shown in Table 1. Further, we classified the policy instruments undertaken to overcome data-sharing barriers by using the NATO framework and substantive-procedural classification (Howlett 1991)

### ***2.3. The development of data sharing initiatives and regulations to promote the adoption of autonomous systems in Singapore***

Being the forerunner in the smart city development after ranking first for three years in a row (from 2018 to 2020) (Smart Nation and Digital Government Office 2022), Singapore has also made strides in testing and adopting various autonomous systems in industrial, transportation, healthcare, and other domains. Singapore has ranked first in the 2020 AV readiness index out of 30 countries with scores for parameters on policy and legislation, technology and innovation, infrastructure, and consumer acceptance (KPMG International 2020). These achievements and timeliness make Singapore a suitable case to be subjected to an in-depth analysis in this study (Yin 2017).

The Smart city mission in Singapore was launched in 2014 to focus on developing three key pillars—digital society, digital economy, and digital government (Smart Nation Singapore 2022). The eGov 2015 Masterplan preceded this to contribute to the ICT infrastructure and provide access to available government data in 2011. The Personal Data Protection Act (PDPA), introduced in 2012, is the law that governs privacy across different sectors in Singapore. Amendments have been made in recent years to impose less stringent requirements on certain provisions to enable regulatory flexibility and encourage innovations deemed important to implementing sandboxes.

With data sharing being a key priority for the Smart Nation vision, the new data.gov.sg was launched in July 2015, comprising high-quality data on the economy, education, environment, finance, health, infrastructure, society, technology, and transport (Gov Tech Singapore 2019). In 2016, the Government Technology Agency (GovTech Singapore) was officially formed under the Smart Nation and Digital Government Office (SNDGO). To work on digitization in public service delivery, the government has published the Digital Government Blueprint as a statement to capitalize on data and use it for new technologies. The first version of the blueprint was published in June 2018, with one of the intentions being to set guidelines for using AI and IoT for operational efficiency (Smart Nation Singapore 2018). In 2019, a government data architecture (GDA) was initiated to lay the grounds for common data standards and formats to enable seamless and efficient data sharing between public agencies to facilitate cross-sector policy analysis and public service delivery in different sectors, including technology trials and deployment (Smart Nation Singapore 2018). The second version was published in December 2020, focusing on identifying the high-impact areas for AI utilization and building on the National AI Strategy introduced in 2019 (Smart Nation Singapore 2020). Specifically, the government intends to build the Smart Nation Sensor Platform and use the sensor data for intelligent operations

(for instance, testing soil quality in plant health monitoring) (Smart Nation Singapore 2020).

To better facilitate data sharing between government agencies, the Public Sector (Governance) Bill was passed in the Singaporean parliament in 2018. To reconcile the potential conflicts between open data sharing practices and the associated legal concerns, the “Trusted data sharing framework” was introduced in 2019. This initiative also responds to concerns about security and trust in data sharing and how these could hamper the benefits that could be capitalized from sharing and analyzing huge volumes of data for AI (IMDA & PDPC 2019). This initiative was curated by the Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC) to provide cross-sectoral guidelines in data sharing, which also applies in novel technology implementation such as autonomous systems and artificial intelligence (AI) tools (IMDA & PDPC 2019). Even though this framework was intended as a preliminary guide for the industry and not to enforce compliance at this point, it serves as a useful medium for data sharing strategy, regulatory considerations, technical and organizational considerations, and ensuring transparency and accountability in data-sharing.

During COVID-19, Singapore introduced smartphone applications for contact tracing and surveillance, which require collecting personal data. The PDPC had to provide notice to inform the public of the purpose of data collection from designated public agencies and the intended use of these data, which is not to be used for purposes other than those authorized by the law (PDPC 2020). The government has introduced standards and references for voluntary compliance for specific autonomous systems like AVs, personal care robots, and industrial and collaborative robots. In governing data sharing in the AV ecosystem, the Land Transport Authority (LTA) in Singapore published a set of documents known as Technical Reference (TR) 68 in early 2019 to offer provisional national standards and guidelines to the AV industry, especially for companies intending to roll-out level 4 and level 5 AVs in mixed-use traffic and on public roads. Singapore Standards Council also published a TR for data sharing between robots, lifts, and automated doorways (TR-93) in 2021, highlighting all necessary protocols. For personal care robots and industrial robots, voluntary standards have been specified by the Council. A recent TR published in 2022 on the safe deployment of robots in the healthcare sector (TR-108) has specifically highlighted protocols for managing sensitive and non-sensitive data of patients.

### **3. Strategies to overcome barriers to data sharing in the adoption of autonomous systems**

This section discusses the strategies the Singapore government uses to overcome barriers to data sharing for autonomous systems that can be extrapolated to other disruptive technologies.

#### **3.1. Overcoming technical barriers**

Technical safety is one of the foremost issues to be prioritized in adopting autonomous systems, especially for autonomous systems with high technological readiness.

Ensuring the safety of autonomous systems would inevitably require some form of data sharing between regulators and technology providers. The deployment of regulatory sandboxes, or testbeds, for autonomous systems is one of the most advanced and important tools to resolve potential contradictions between technological innovation and regulatory compliance. It can also ensure that technical barriers to data sharing can be addressed more dynamically. For instance, in Singapore's autonomous vehicles (AV) deployment, the regulatory sandbox is implemented as a "soft" risk management experimental tool to govern various technological risks that may arise from AV implementation (Tan and Taeihagh 2021). The current rules oblige private AV developers to share data and information on all forms of accidents and incidents of malfunctions that involve deaths or injuries (Road Traffic Act (Chapter 276): Road Traffic (Autonomous Motor Vehicles) Rules 2017; Road Traffic Act 2017). This regulatory sandbox is intended to be effective for only five years, after which permanent regulations would be enacted, informed by the learnings acquired during various AV trials (Tan & Taeihagh 2021).

For the movement of automated guided vehicles and autonomous mobile robots in lifts and buildings, a system architecture for data exchanges for robot-to-robot and robot-to-lift has been specified (TR 93, 2021). The required data exchanges between the servers of the lifts and robots have to be specified with time stamps to enable the collection and preservation of data in recognized data formats as listed in the TR.

Likewise, in healthcare, the deployment of robotics and autonomous systems involves the establishment of testbeds and living laboratories which mimic a sandbox approach like the AVs. In Singapore, the Center for Healthcare Assistive and Robotics Technologies (CHART) functions as both a sandbox and an implementation task force to optimize automation processes in deploying healthcare robotics and autonomous systems (Tan & Taeihagh 2021). In addressing potential technical barriers to data sharing, Robotics Middleware for Healthcare (RoMi-H) has been established to facilitate data sharing by integrating diverse systems in the Singapore Public Healthcare Institutions, which include robotic systems, medical devices, IoT devices, Hospital Information Systems, nurse/operator user interface devices and building infrastructures. Fundamentally, RoMi-H is intended to enhance interoperability and increase operational efficiency in healthcare settings by acting as a central communication channel that facilitates diverse systems to work on a unified platform (CHART 2021). For robots in healthcare settings, a data management plan must be created and defined for usage, storage, and management of data points when specifying the task of robots (TR 108, 2022).

By and large, Singapore has attempted to address the overarching technical barriers to data sharing in the "Trusted Data Sharing Framework" launched in 2019. The "Trusted Data Sharing Framework" stipulates the roles of different actors in a data sharing ecosystem (i.e. data suppliers, data service providers, authority, data consumers), lays out data sharing trust principles, and proposes three data sharing models (bilateral, multilateral, and decentralized) and prescribes guidelines for different stakeholders to standardize their respective data sharing agreements (IMDA & PDPC 2019).



With the policy intention to facilitate data sharing across various autonomous systems to achieve smart city mission in Singapore centering on digital society, digital economy and digital government, a combination of authority and nodality tools that are both substantive- and procedural-based were deployed. Beyond the light-touch regulation observed in the sandbox of autonomous vehicles, most of the tools function to provide sufficient data sharing information necessary to accelerate the development of autonomous systems in Singapore.

### **3.2. Overcoming motivational barriers**

To counteract the problem of disagreement in data use, the “Trusted Data Sharing Framework” has recommended various actors to follow these seven strategies in the formulation of data sharing agreements, which include (i) granting of license/permissions to use data for the intended purpose, (ii) setting restrictions, warranties or other assurances provided in relation to the “Data Providers” rights in the data, (iii) specifying liability for contract breaches between parties, (iv) maintaining confidentiality, (v) deciding on the term/duration of contract agreement, (vi) legislations and resolving disputes, and (vii) reflecting on the technical considerations for data sharing (IMDA & PDPC 2019).

The Singapore government launched its government data strategy in 2018 to break down the motivational barriers and resistance among different public agencies to share data (Tay 2020). GDA compiles datasets across four domains of government data—individual, business, geospatial, and sensor data (Singapore Public Service 2020). One of the public agencies that uses the GDA dataset the most is GovTech’s Data Science and Artificial Intelligence Division (Singapore Public Service 2020). Between the public and private sectors, another initiative known as Core Operations Development Environment and eXchange (CODEX) was started as a shared digital platform to enable data sharing. CODEX aims to shift less sensitive public data to commercial cloud services and tap into the private sector to develop digital solutions that improve public service delivery. In addition, a Singapore Government Technology Stack (SGTS) that comprises a suite of shared software components and infrastructure was also started as part of CODEX initiatives to enable government and businesses to collaborate more efficiently in building various digital applications. The current data sharing arrangement allows the public and private sectors to share reusable digital components, including machine-readable data, microservices, and middleware (Smart Nation and Digital Government Office 2022).

The TR68 is a crucial policy document to steer the development and deployment of AVs in Singapore. Specifically, part four of the TR68 specifies vehicular data types and formats for the following purposes in data sharing: (i) data to be recorded by the data storage system for automated driving, (ii) reasonable and adequate use of AV data to continuously improve safety, (iii) management of dynamic content (high definition maps and road traffic conditions), (iv) reporting of accidents and claim disputes, and (v) vehicle to everything information exchange to enhance safety and efficiency (Roy 2019). In addition to providing clear guidelines, these standards help to lower the opportunity cost for existing and prospective AV developers to launch



their AV trials in an open but prescriptive regulatory environment such as Singapore (Tan and Taeihagh 2021). For industrial robots, the standards specify that data for safety-related control systems must be included in the information for users, ensuring that manufacturers incorporate all required data (SS ISO 10218-22 2016).

A combination of authority, nodality and organisation tools were deployed to incentivise data sharing behavior and promote public-private data sharing initiatives to overcome motivational barriers in data sharing. These tools are both substantive- and procedural-based, functioning as soft-laws, information providers and collaborative platform to encourage data sharing.

### **3.3. Overcoming economic barriers**

In Singapore, strong financial incentives exist to promote the adoption of new technological frontiers in data sharing for autonomous systems and other AI applications, such as machine learning technologies and privacy-preserving technologies (AI Singapore 2020; Shiao 2019).

To address regulatory barriers in cross-border data sharing, Singapore works with international partners to develop as well as invest in machine learning techniques such as federated learning to enable different parties to train AI models without having to exchange raw data (AI Singapore 2020). Likewise, significant research investment in privacy-preserving analytics across various smart technologies and autonomous systems have been made for two leading universities in Singapore (National University of Singapore and Nanyang Technological University) to develop innovative solutions that enhance data sharing capabilities to minimize the risk of privacy breach, aside from promoting the training of skilled manpower (Shiao 2019).

Treasury is the most dominant tool deployed in overcoming economic barriers to strengthen data sharing capabilities, in addition to safeguarding data security in the implementation of disruptive technology in Singapore. The treasury tools deployed are largely substantive-based to provide direct investments to the technologies tested.

### **3.4. Overcoming political barriers**

Clear policies or guidelines are of paramount importance to improve trust among the users to share their data and for data collectors to use the data responsibly. The standards for personal care robots specify that data display items in robots be easily understood by users to avoid any confusion in human-robot interaction (SS ISO 13482, 2017). This will build trust between users and providers of data. More broadly, the Monetary Authority of Singapore launched a whitepaper in 2021 to lay down the four foundational pillars to guide industries in building robust digital infrastructures and guide the design of digital identity across different sectors. This whitepaper elaborates on the seven important principles to facilitate responsible data exchange between data collectors and end-users (Monetary Authority of Singapore 2021). For authorization and consent, it proposes that data collectors need to be upfront to the end-users about the extent to which their personal data would be used, shared, or published, and these should be communicated transparently. In addition, security of

information needs to be upheld, and good data minimization practices—which necessitate the collection, use and storing of only data that are required to create or provide a service—should be encouraged. Furthermore, consent services should be presented transparently in a dashboard or data vault to provide end-users clear information on what data would be used, to whom it would be disclosed, for what purposes and the duration to which the consent is valid. The dashboard or data vault should be designed to allow individuals to log in anytime to change their settings and level of permissions, including adding new services with which to share their data.

Beyond the provision of guidelines, Singapore has also grown its capabilities in building trust in digital technology deployment. More recently, in June 2022, the Minister for Communications and Information in Singapore announced a \$50 million investment from IMDA and the National Research Foundation to fund the development of a Digital Trust Center (DTC)—a research center to be hosted by Nanyang Technological University. It will focus on developing four key areas of trust technologies, including trust tech research, trust tech innovation, new sandbox environment for businesses and deepening local capabilities in digital trust (EDB and Singapore 2021).

To overcome political barriers in data sharing, the government deployed a combination of nodality and treasury tools to strengthen the industry’s trust in data sharing and develop trust technologies. These tools are largely substantive-based, existing in the forms of direct financial investment and information sharing guidelines.

### **3.5. Overcoming legal barriers**

Currently, organizations and entities can apply for data sharing arrangements to be exempted from one or more obligations of the PDPA on a case-by-case basis (Personal Data Protection Commission of Singapore, 2022). The PDPC also produced a data sharing guide to explain factors to consider before sharing data, ways to facilitate data sharing within the organization, between or among organizations and with a data intermediary, risk assessment and mitigation, as well as different ways of obtaining consent (Personal Data Protection Commission of Singapore, 2018). The Trusted Data Sharing Framework also provided supplementary guidelines for data sharing (IMDA & PDPC 2019).

In the case of autonomous vehicles, the Singapore Road Traffic Act 2017 for Autonomous Motor Vehicles, modified in 2020, has laid the foundation for data sharing obligations for AV developers. Specifically, the provisions clearly state that “data should always be recorded,” even when AV technology is not in operation, and data must be collected in the format specified by the authority and kept for at least three years. The types of data to be collected are also specified. The law amendment also requires AV developers to always keep records, especially when AV malfunctions or in AV incidents involving personal injury or property damage. In the provision, data cannot be edited, and copies must be provided to the authority. Penalty in the form of fines will be imposed, with the amount doubled in the case of a second and subsequent conviction (Singapore Statutes Online 2022).

For robots in healthcare, The TR specifies storage and transmission of data. Stakeholders have to identify whether data are classified as sensitive (for example patient health, data that is confidential to a health center or data covered under statutory and regulatory requirements) or non-sensitive (instructions or patient requests) and determine storage (temporary, short-term, or permanent)(TR 108, 2022). Additionally, the treatment of data must be specified in the form of transmission (whether the data is not to be transmitted to a robot for use, and if it is transmitted, it is wireless transmission through encryption or via an open network) (TR 108, 2022).

Authority is the most notable tool deployed to codify hard and soft laws in overcoming legal barriers in data sharing. They are both substantive- and procedural-based, aiming to provide direct information as well as streamlining the process required for exemption from certain legal obligations of data privacy protection.

### **3.6. Overcoming ethical barriers**

Ethical barriers in data sharing often manifest as a lack of proportionality (through assessment of the risks and benefits from the amount and type of data requested) and a lack of reciprocity (lack of credits given to data producers/suppliers) (Van Panhuis et al. 2014). These issues could lead to safety concerns in operating autonomous systems and potential exploitation of goodwill from the data producers. For instance, in governing the safety of autonomous vehicles, regulators and AV developers are confronted with the issue of a moral dilemma which can be interpreted differently due to the interaction of personal moral philosophy as well as the broader culture in the society (Rhim et al. 2021; Ryan, Murphy, and Mullins 2020). These factors have far-reaching implications in influencing how crash algorithms are designed to prioritize the safety of certain social groups of people, while inevitably predisposing other social groups to a higher risk of dying in collisions when autonomous vehicles are forced to make a choice on how to swerve in an unavoidable accident. While there have been recommendations and guidelines across the world, to date, the regulations are still largely nebulous, and decisions were often made to result in the least likely determinable harm (Ryan, Murphy, and Mullins 2020). To overcome safety risks and maintain proportionality, the LTA, since 2016, has required all AVs to be used for trials to demonstrate trustworthiness and pass safety assessments before proceeding with the trials. There are also specific data sharing or data-related requirements drafted as soft laws that need to be fulfilled before AVs can proceed with the trials. These include having liability insurance, equipping each AV with a data recorder capable of storing information during use and storing basic data, including date, time, location, speed, front- and rear-facing imaging in digital format and keeping these data for at least three years. Any such authorized person must keep records of and notify the authority of all incidents and accidents. Lastly, a failure alert system must be installed to allow the driver to take immediate manual control in an emergency (Singapore Academy of Law Law Reform Committee & Constantine S 2020). In the case of another type of autonomous system in healthcare, such as when designing robotic pets for older people, robot designers have been confronted with

several ethical issues such as deception and objectification of older people. For instance, when interacting with these robotic pets, older people with cognitive decline or cognitive issues may be misled to think that they are interacting with real pets, and these false impressions could potentially undermine their dignity or counterfeit authentic social engagement. There are philosophical debates and value tensions that occur as to whether authenticity should be upheld or the overall well-being of older people should be prioritized in the process of care and how would the choice influence the extent of “information or data” that ought to be shared with the care recipients. In Singapore, these ethical barriers to data sharing have been recognized by the stakeholders, and focus has been on ensuring more transparent communications between caregivers and the care recipients when deploying these technologies in various care settings (Tan and Taelhagh 2020). Table 2 summarizes the strategies taken to overcome barriers to data sharing in the implementation of autonomous systems in Singapore. Some of these strategies are specific to autonomous systems while others are broader strategies that apply to a variety of disruptive technologies.

Intending to create standards for data sharing to address ethical issues in the implementation of autonomous vehicles, substantive-based nodality tool is the most dominant tool deployed. It appears in the form of guidelines, helping the developers and regulators to learn and adapt the guidelines to emerging situations as the technology matures.

#### **4. Lessons for practice: a multi-pronged approach in promoting collaborative and responsible data sharing for novel technology adoption**

Using the insights from strategies discussed in the previous section, this section provides lessons for a holistic approach to promoting collaborative and responsible data sharing practices for adopting disruptive technologies.

##### **4.1. Addressing technical barriers**

Regulatory sandboxes or living laboratories are instruments effective for experimenting with novel technologies by allowing room for a margin of errors to occur. More importantly, they allow novel technologies to be tested in a controlled regulatory environment to assess various aspects of their safety and cybersecurity and to balance innovations with privacy concerns (Tan and Taelhagh 2020, Tan & Taelhagh 2021). When deploying regulatory sandboxes, the governments need to promote proactive regulatory enforcement by having explicit provisions for data sharing, including stipulating the types, nature, and duration of data to be shared by the developers.

As data sharing is key to accelerating novel technology adoption and promoting digital transformation, sandbox approaches can also be used to develop emerging tools and technologies that explore innovative approaches to data sharing, investigating socio-technical factors that promote data sharing without violating the privacy laws (Granell et al. 2022).

**Table 2.** Strategies taken to overcome different types of barriers to data sharing in the implementation of autonomous systems and disruptive technologies in Singapore.

Data sharing barriers	Specific strategies for autonomous systems and generic strategies for disruptive technologies	Intended policy objectives	Types of policy tools deployed
Technical	<p>Specific strategies for autonomous systems:</p> <ul style="list-style-type: none"> <li>• Autonomous vehicles: Regulatory sandbox necessitates private AV developers to share data and information on all forms of accidents and incidents of malfunctions that involve deaths or injuries.</li> <li>• Autonomous robots and automated guided vehicles in construction: A system architecture for data exchanges for robots to robots and robots to lift was designed.</li> <li>• Robotics in healthcare: Robotics Middleware for Healthcare (RoMi-H) was established to facilitate data sharing by integrating diverse information and device systems in the hospitals.</li> </ul> <p>Generic strategy for disruptive technologies:</p> <ul style="list-style-type: none"> <li>• The 'Trusted Data Sharing Framework' launched in 2019 stipulates the roles of different actors in a data sharing ecosystem, lays out data sharing trust principles, proposes three data sharing models and prescribes guidelines to standardize different data sharing agreements.</li> </ul>	Facilitating data sharing in various autonomous systems to achieve smart city mission.	Authority, nodality, procedural-based.
Motivational	<p>Specific strategies for autonomous systems:</p> <ul style="list-style-type: none"> <li>• Autonomous vehicles: A policy document (TR68) was launched to provide comprehensive guidelines to the AV industry. Part four of the document specifies vehicular data types and formats for data sharing under different circumstances.</li> </ul> <p>Generic strategies for disruptive technologies</p> <ul style="list-style-type: none"> <li>• Provisions for data sharing agreements from the 'Trusted Data Sharing Framework' launched in 2019.</li> <li>• Different initiatives started to facilitate data sharing within the public domain and between the public and private sectors. Major initiatives include GDA (compiles datasets across four domains of government data—individual, business, geospatial and sensor data), CODEX (shared digital platform to enable data sharing between public and private sectors) and SGTs (allows public and private sectors to share reusable digital components including machine</li> </ul>	Incentivising data sharing behavior and promoting public-private data sharing initiatives.	Authority, nodality, organization, substantive- and procedural-based.

*(continued)*

**Table 2.** Continued.

Data sharing barriers	Specific strategies for autonomous systems and generic strategies for disruptive technologies	Intended policy objectives	Types of policy tools deployed
Economic	<p>readable data, microservices and middleware).</p> <p>Generic strategies for disruptive technologies</p> <ul style="list-style-type: none"> <li>• Singapore works with international partners to develop as well as to invest in machine learning techniques to facilitate cross-border sharing.</li> <li>• Research investment to develop innovative solutions that enhance data sharing capabilities.</li> </ul>	Strengthening data sharing capabilities.	Treasury, substantive-based.
Political	<p>Generic strategies for disruptive technologies</p> <ul style="list-style-type: none"> <li>• A whitepaper was launched by MAS to lay down the four foundational pillars to guide industries in building robust digital infrastructures and to guide the design of digital identity to build trust in data sharing.</li> <li>• The government funded the development of a Digital Trust Center to focus on developing four key areas of trust technologies (i.e. trust tech research, trust tech innovation, new sandbox environment for businesses, and deepen local capabilities in digital trust).</li> </ul>	Strengthening trust in data sharing and developing trust technologies.	Nodality and Treasury, substantive-based.
Legal	<p>Specific strategies for autonomous systems</p> <ul style="list-style-type: none"> <li>• Autonomous vehicles: The Singapore Road Traffic Act 2017 for Autonomous Motor Vehicles, modified in 2020 has laid down the foundation for data sharing obligations for AV developers.</li> <li>• TR 108 specifies the classification of data as sensitive or non-sensitive and the requirement of rules for the storage and transmission of data for robots deployed in healthcare settings.</li> </ul>	Codifying hard and soft laws to increase the clarity of data sharing.	Authority, substantive- and procedural-based
Ethical	<p>Generic strategy for disruptive technologies</p> <ul style="list-style-type: none"> <li>• Entities can now apply for data sharing arrangements to be exempted from one or more obligations of the PDPA on a case-by-case basis.</li> </ul> <p>Specific strategy for autonomous systems</p> <ul style="list-style-type: none"> <li>• Autonomous vehicles: To uphold safety during the AV trials, specific data sharing or data-related requirements have been specified, and developers will need to fulfill these requirements before their AVs can proceed with the trials.</li> </ul>	Creating standards for data sharing in autonomous systems.	Nodality, substantive-based.

## **4.2. Addressing motivational barriers**

In encouraging public-private collaborations in the technology space to address motivational barriers in data sharing, much can be learned from the tradition of public-private partnerships in the pharmaceutical industry to promote drug development and discovery. One notable example is the involvement of leading pharmaceutical companies and public organizations that have joined the World Intellectual Property Organization (WIPO) to establish a consortium that offers different mechanisms to share intellectual property that has the potential to be used in new drug discovery and development of more effective products to treat neglected diseases across the world (Davis et al. 2021). To date, WIPO has resulted in more than 140 public-private collaborations, with the majority concentrated on research and development (ibid.). The technology industry can emulate this experience and establish a consortium to share big data or even intellectual properties for certain aspects of the technology, especially when these collaborations have the potential to promote equity in access to autonomous systems and disruptive technologies for developing countries. Jean-Quartier et al. (2022) investigated the factors that lead to collaborative use and data exchange among stakeholders, including public agencies, academia, and the private sector. They concluded that open data policies, common workshops, conducting workshops, integration with international channels and public grants are enablers that facilitate data exchange and cooperation among these stakeholders.

Beyond data sharing, there can also be increased effort to encourage knowledge transfer and increased data use and reuse between public and private actors in different machine learning settings, such as federated learning and transfer learning. In a federated learning environment, machine learning algorithms are trained collaboratively across different parties in a decentralized manner without explicit data exchange to enable collective learning. Likewise, a transfer learning setting also allows a machine learning model to be trained in one dataset before applying it to train on other datasets owned by different owners without direct exchange of data (Jean-Quartier et al. 2022).

## **4.3. Addressing economic barriers**

To overcome economic barriers to data sharing, it is inevitable that the government ramp up resources, including manpower and analytical capacity, to promote data sharing between various entities. For instance, a viable strategy is investing in privacy-preserving technologies to facilitate safe and accountable data sharing between and across different public agencies and private entities. One such technology which has witnessed a significant rate of annualized growth in user rates is the fully homomorphic encryption (FHE) which encrypts the data before sharing them, enabling the external party to analyze the data without decoding them (Farrall et al. 2021). There are also other privacy-preserving technologies that function differently, such as differential privacy (adding noise to the data to prevent reverse-engineering of the original inputs), functional encryption (allowing selected users to view certain parts of the encrypted text with a special key) and federated analysis (sharing insights from the analysis without sharing the original data) (Farrall et al. 2021; Zanussi 2021).



While adopting these technologies is not a magic bullet for the government to be shielded from data violations or breaches, they can pave the way to a more secure data sharing environment alongside other policy and regulatory safeguards.

#### **4.4. Addressing political barriers**

To address political barriers to data sharing, setting provisional standards and guidelines in data sharing agreements between public agencies or between public and private sectors is useful to reduce the opportunity cost of data sharing. Besides the Trusted Data Sharing Framework in Singapore, the OECD Council has also developed recommendations to enhance access to and sharing of data to provide preliminary guidelines for data sharing arrangements between different actors and stakeholders (OECD 2021a). Another illuminating example of a country that has provided comprehensive policy guidelines to facilitate data sharing to advance technology adoption is the data management framework for collaborative data utilization launched by Japan's Ministry of Economy, Trade and Utilization (METI). Released in April 2022, this framework identifies risks through the data lifecycle from data generation/acquisition to data processing/use, to data transfer, to data storage, to data disposal, and prescribing various measures to promote data security when the data attributes change in different stage of the lifecycle. Furthermore, the framework also considers the perspective of laws in different jurisdictions, internal rules of the organizations, and contracts between organizations and encompass attributes such as data category, disclosure scope, purpose of use, data management entity and data right holder (One Trust Data Guidance 2022).

#### **4.5. Addressing legal barriers**

The strict provisions in privacy laws in most jurisdictions are seen as one of the most significant barriers to data sharing and are perceived as stifling to the promotion of technological innovation. One option to lessen the tension between these two realms is to enable flexibility in the governance of privacy law and exemption of certain obligations for technology companies through special data sharing arrangements like what Singapore has done with the PDPA. In doing so, governments and legislators should lay out the steps and mechanisms, including the inclusion criteria for such exemption to be considered. Furthermore, the Covid-19 pandemic has also highlighted the need for some exemptions when enforcing privacy laws in situations whereby data sharing between citizens and government, as well as between private and public agencies, is inevitable to safeguard public health and/or when there is a utilitarian intent to rush the research and development processes of potentially life-saving health innovations capable of controlling the pandemic (Newlands et al. 2020).

#### **4.6. Addressing ethical barriers**

Adopting disruptive technologies comes with unique risks and benefits in their operation. A thorough ethical analysis for all novel technologies needs to be formalized at

the stage when they are still in their pilot phases. This will help determine the extent of data sharing provisions that technology companies must abide when piloting their prototypes or technological solutions. Apart from ethical analysis, there have also been calls for technology companies to adopt “ethics by design” in their technology solutions. This notion refers to embedding ethical principles in developing and designing technology and allowing procedures to uphold legal and ethical compliance by default (Viberg Johansson, Bentzen, and Mascalzoni 2022). Table 3 highlights the lessons for policymakers and practitioners on how to promote collaborative and responsible data sharing for disruptive technologies such as autonomous systems and overcome data sharing barriers.

## 5. Conclusion

By examining the experiences of governing data sharing for autonomous systems in Singapore, we identified a slew of specific strategies for autonomous systems and generic strategies for disruptive technologies that both public and private agencies can adopt to overcome different types of barriers to data sharing. Specific strategies that autonomous systems could implement to address the different extent and nature of barriers to data sharing include setting up a sandbox environment or a living

**Table 3.** Lessons for policymakers and industry practitioners to promote collaborative and responsible data sharing for autonomous systems and disruptive technologies.

Data sharing barriers	Recommendations for addressing data sharing barriers
Technical	<p>Promoting data sharing within regulatory sandboxes for autonomous systems and using sandboxes to explore innovative approaches of data sharing for novel technologies</p> <ul style="list-style-type: none"> <li>• Promote proactive regulatory enforcement by having clear provisions for data sharing (data types, nature, and duration of data to be shared by the developers) (Tan and Taeihagh 2021).</li> <li>• Use the sandbox approach to identify innovative data-sharing approaches without violating privacy laws (Granell et al. 2022).</li> </ul>
Motivational	<p>Promoting public-private collaborations in data sharing and knowledge transfer</p> <ul style="list-style-type: none"> <li>• Emulate the pharmaceutical industry to establish a consortium that offers different mechanisms to share big data or even intellectual properties with the potential to promote equity in access to autonomous systems and disruptive technology adoption for developing countries (Davis et al. 2021; Jean-Quartier et al. 2022).</li> <li>• Encourage knowledge transfer and increased data use and reuse between public and private actors in different machine learning settings (Jean-Quartier et al. 2022).</li> </ul>
Economic	<p>Ramping up resources and analytical capacity to adopt privacy-preserving technologies</p> <ul style="list-style-type: none"> <li>• Invest in privacy-preserving technologies to facilitate safe and accountable data sharing between and across different public agencies and private entities (Zanussi 2021; Farrall et al., 2021).</li> </ul>
Political	<p>Producing data sharing policy guidelines</p> <ul style="list-style-type: none"> <li>• Produce comprehensive policy guidelines on data sharing framework.</li> </ul>
Legal	<p>Allowing discretion toward privacy laws to be exercised under unique circumstances as well as under emergencies</p> <ul style="list-style-type: none"> <li>• Governments and legislators should lay out the steps and mechanisms, including the inclusion criteria for circumstances in which certain provisions from the national privacy law can be exempted from enforcement (Newlands et al. 2020).</li> </ul>
Ethical	<p>Formalising thorough ethical analysis and ‘ethics by design’ for novel technologies to address unique ethical dilemmas</p> <ul style="list-style-type: none"> <li>• Enforce a thorough ethical analysis for all autonomous systems and disruptive technology before they go into trials, and this should include stipulating the extent of data sharing provisions that technology companies need to abide (Viberg Johansson, Bentzen, and Mascalzoni 2022).</li> </ul>

laboratory to overcome technical barriers; providing explicit guidance as well as promoting knowledge transfer and public-private collaborations to resolve motivational barriers; using an ethical analysis or an “ethics by design” approach address ethical barriers; and allowing discretionary or circumstantial provisions for privacy laws to tackle legal barriers. While there are currently no specific strategies for autonomous systems in overcoming economic and political barriers to data sharing, the broader strategies used for adoption of disruptive technologies in Singapore suggest expansion of resources along with building capacity and trust to help with promoting a more open and dynamic data sharing ecosystem to better address the economic and political barriers.

One critical insight in policy design that could be derived from Singapore’s experience in facilitating data sharing for autonomous systems is the importance of information-based nodality tools to fast-track technology implementation. Not only do nodality tools provide information clarity to all the actors in the technology ecosystem, but they also minimize information asymmetry between the regulators and technology developers as far as safety and liability are concerned. While nodality is the most dominant tool deployed to overcome technical, motivational, political, and ethical barriers, the government has used a combination of nodality, authority, treasury, and organization tools overall.

As smart city developments across the world fuel the expansion of disruptive technologies, our study calls for future research to analyze innovative reform strategies taken to address challenges in data sharing in the context of disruptive technologies such as autonomous systems in other jurisdictions. In addition, identifying opportunities and strategic needs for data sharing will also help to improve the culture of building an open data policy for such disruptive technologies. The Covid-19 pandemic has also brought the importance of governing data sharing to the front and center of the governments’ agenda, especially greater alignment and balance between governing data privacy and upholding good public health practices are warranted. As such, comparing policy lessons worldwide, including examining the instruments that govern data sharing practices in autonomous systems and other disruptive technologies will be a promising future research agenda.

## **Acknowledgments**

Araz Taeihagh is grateful for the support provided by the Lee Kuan Yew School of Public Policy, National University of Singapore.

## **CRedit authorship statement**

Conceptualization, A.T.; methodology, S.-Y.T and A.T.; validation, A.T.; formal analysis, S.-Y.T, and A.T.; investigation, S.-Y.T, A.T and D.P.; resources, A.T.; data curation, S.-Y.T, A.T. and D.P.; writing and editing S.-Y.T, A.T. and D.P.; supervision, A.T.; project administration, A.T.; funding acquisition, A.T. All authors read and agreed to the published version of the manuscript.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Funding

This research is supported by Ministry of Education Singapore AcRF Tier 1 funding support (A-0003287-00-00) and the Lee Kuan Yew School of Public Policy, National University of Singapore (A-0003990-00-00).

## ORCID

Araz Taeihagh  <http://orcid.org/0000-0002-4812-4745>

## References

- Abu-Elkheir, M., M. Hayajneh, and N. A. Ali. 2013. "Data Management for the Internet of Things: Design Primitives and Solution." *Sensors* 13 (11): 15582–15612. doi:10.3390/s131115582.
- AI Singapore. 2020. "AI Singapore's Journey into the World of Federated Learning." AI Singapore, October 20. <https://aisingapore.org/2020/10/ai-singapores-journey-into-the-world-of-federated-learning/>.
- Lim, H., & Taeihagh, A. (2018). Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies*, 11(5), 1062. <https://doi.org/10.3390/en11051062>
- Lim, H. S. M., & Taeihagh, A. (2019). Algorithmic Decision-Making in AVs: Understanding Ethical and Technical Concerns for Smart Cities. *Sustainability*, 11(20), 5791. <https://doi.org/10.3390/su11205791>
- Tan, S. Y., & Taeihagh, A. (2021). Governing the adoption of robotics and autonomous systems in long-term care in Singapore. *Policy and Society*, 40(2), 211–231.
- Pande, D., & Taeihagh, A. (Forthcoming). Governance of artificial agency.
- CHART. 2021. "Robotics Middleware for Healthcare (RoMi-H)." <https://www.cgh.com.sg/chart/Documents/RoMi-H%20CHART%20Framework.pdf>.
- Davis, A. M., O. Engkvist, R. J. Fairclough, I. Feierberg, A. Freeman, and P. Iyer. 2021. "Public-Private Partnerships: Compound and Data Sharing in Drug Discovery and Development." *SLAS Discovery* 26 (5): 604–619. doi:10.1177/2472555220982268.[PMC].
- EDB, Singapore. 2021. "Singapore: Southeast Asia's Testbed for Smart City Solutions." May 11. <https://www.edb.gov.sg/en/business-insights/insights/singapore-southeast-asia-s-testbed-for-smart-city-solutions.html>,
- Falco, G. 2020. "A Smart City Internet for Autonomous Systems." 2020 IEEE Security and Privacy Workshops (SPW), 215–220, San Francisco, CA, USA.
- Farrall, F., N. Mittal, C. Narra, and J. Tello. 2021. "Data-Sharing Made Easy." Deloitte Insights, December 7. <https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/data-sharing-technologies.html>.
- Finn, R. L., D. Wright, and M. Friedewald. 2013. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, 3–32. Springer, Dordrecht.
- Frost, A. 2019. "World's First Retrofitted Autonomous Pickup Truck to Start Trials in Australia Next Year." <https://www.traffictechnologytoday.com/news/autonomous-vehicles/worlds-first-retrofitted-autonomous-pickup-truck-to-start-trials-in-australia-next-year.html>
- Glancy, D. J. 2012. "Privacy in Autonomous Vehicles." *Santa Clara Law Review* 52: 1171.
- Gov Tech Singapore. 2019. "Factsheet Data.gov.sg." <https://www.tech.gov.sg/files/products-and-services/Datagovsg-Factsheet-0319.pdf>.

- Granel, C., P. Mooney, S. Jirka, M. Rieke, F. Ostermann, J. Van Den Broecke, A. Sarretta, S. Verhulst, L. Dencik, and H. Oost. 2022. "Emerging Approaches for Data-Driven Innovation in Europe: Sandbox Experiments on the Governance of Data and Technology", European Commission, Joint Research Centre, Publications Office of the European Union, 2022, 10.2760/630723
- Hawkins, A. J. 2019. "Mercedes-Benz and Bosch Are Testing Self-Driving Taxis in San Jose." <https://www.theverge.com/2019/12/9/21002911/mercedes-benz-bosch-self-driving-taxi-car-class-san-jose-autonomous>.
- Howlett, M. 1991. "Policy Instruments, Policy Styles, and Policy Implementation: National Approaches to Theories of Instrument Choice." *Policy Studies Journal* 19 (2): 1–21. doi:10.1111/j.1541-0072.1991.tb01878.x.
- IMDA & PDPC. 2019. "Trusted Data Sharing Framework." <https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf>.
- Jean-Quartier, C., M. Rey Mazón, M. Lovrić, and S. Stryeck. 2022. "Collaborative Data Use between Private and Public Stakeholders—a Regional Case Study." *Data* 7 (2): 20. doi:10.3390/data7020020.
- KPMG International. 2020. "2020 Autonomous Vehicles Readiness Index." <https://home.kpmg/xx/en/home/insights/2020/06/autonomous-vehicles-readiness-index.html>
- Leikas, J., R. Koivisto, and N. Gotcheva. 2019. "Ethical Framework for Designing Autonomous Intelligent Systems." *Journal of Open Innovation* 5 (1): 18. doi:10.3390/joitmc5010018.
- Liang, W., G. A. Tadesse, D. Ho, F.-F. Li, M. Zaharia, C. Zhang, and J. Zou. 2022. "Advances, Challenges and Opportunities in Creating Data for Trustworthy AI." *Nature Machine Intelligence* 4 (8): 669–677. doi:10.1038/s42256-022-00516-1.
- Lim, H., and A. Taeihagh. 2018. "Autonomous Vehicles for Smart and Sustainable Cities: An in-Depth Exploration of Privacy and Cybersecurity Implications." *Energies* 11 (5): 1062. doi:10.3390/en11051062.
- McCarthy, N. 2009. "Autonomous Systems: Social, Legal and Ethical Issues." Royal Academy of Engineering (Great Britain). (2009). London, UK. [http://www.raeng.org.uk/news/publications/list/reports/Autonomous\\_Systems\\_Report\\_09.pdf](http://www.raeng.org.uk/news/publications/list/reports/Autonomous_Systems_Report_09.pdf)
- Monetary Authority of Singapore. 2021. "Foundational Digital Infrastructures for Inclusive Digital Economies." <https://www.mas.gov.sg/-/media/MAS/Fintech/FDI/Foundational>
- Newlands, G., C. Lutz, A. Tamò-Larrieux, E. F. Villaronga, R. Harasgama, and G. Scheitlin. 2020. "Innovation under Pressure: Implications for Data Privacy during the Covid-19 Pandemic." *Big Data & Society* 7 (2): 205395172097668. doi:10.1177/2053951720976680.
- Nissenbaum, H. 2004. "Privacy as Contextual Integrity." *Washington Law Review* 79: 119.
- OECD. 2021a. "Data Governance: Enhancing Access to and Sharing of Data – OECD." <https://www.oecd.org/sti/ieconomy/enhanced-data-access.htm>.
- OECD. 2021b. "Legal Instruments." October 6. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>.
- One Trust Data Guidance. 2022. "Japan: METI Releases Data Management Framework for Collaborative Data Utilisation." DataGuidance, April 11. <https://www.dataguidance.com/news/japan-meti-releases-data-management-framework>
- PDPC. 2020. "PDPC | Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry." April 24. <https://www.pdpc.gov.sg/Help-and-Resources/2020/03/Advisory-on-Collection-of-Personal-Data-for-COVID-19-Contact-Tracing>.
- PDPC. 2022. Personal Data Protection Commission. Data Sharing Arrangements. Singapore, 20 July 2022. <https://www.pdpc.gov.sg/overview-ofpdpa/the-legislation/exemption-requests/data-sharing-arrangements>
- PricewaterhouseCoopers. 2021. "Powering Safe and Trusted Data Sharing in Singapore." PwC, August. <https://www.pwc.com/sg/en/publications/powering-safe-and-trusted-data-sharing-in-singapore.html>.
- Radu, L.-D. 2020. "Disruptive Technologies in Smart Cities: A Survey on Current Trends and Challenges." *Smart Cities* 3 (3): 1022–1038. doi:10.3390/smartcities3030051.

- Raso, F. A., H. Hilligoss, V. Krishnamurthy, C. Bavitz, and L. Kim. 2018. *Artificial Intelligence & Human Rights: Opportunities & Risks*. Berkman Klein Center Research Publication, 2018–2016. Harvard, USA.
- Ray, P. P. 2016. “Internet of Robotic Things: Concept, Technologies, and Challenges.” *IEEE Access* 4: 9489–9500. doi:10.1109/ACCESS.2017.2647747.
- Rhim, J., J.-H. Lee, M. Chen, and A. Lim. 2021. “A Deeper Look at Autonomous Vehicle Ethics: An Integrative Ethical Decision-Making Framework to Explain Moral Pluralism.” *Frontiers in Robotics and Artificial Intelligence* 8: 632394. doi:10.3389/frobt.2021.632394.
- Ridden, P. 2019. “Wayve to Start Autonomous Car Trials in London.” <https://newatlas.com/automotive/wayve-autonomous-car-trials-central-london/>
- Road Traffic Act. 2017. (Chapter 276): Road Traffic (Autonomous Motor Vehicles) Rules 2017. Singapore, (testimony of K. K. Pang).
- Roy, S. 2019. “How the LTA’s TR68 Fuelled Singapore’s Autonomous Vehicle Agenda.” *Tech Wire Asia*, March 7. <https://techwireasia.com/amp/2019/03/how-the-ltas-tr68-fuelled-singapore-autonomous-vehicle-agenda/>.
- Russo, M., and T. Feng. 2020. *The Risks and Rewards of Data Sharing for Smart Cities*. BCG Henderson Institute, 7. Boston, Massachusetts, USA.
- Ryan, C., F. Murphy, and M. Mullins. 2020. “Spatial Risk Modelling of Behavioural Hotspots: Risk-Aware Path Planning for Autonomous Vehicles.” *Transportation Research Part A: Policy and Practice* 134: 152–163. <https://doi.org/10.1016/j.tra.2020.01.024>
- Shiao, V. 2019. “Two New Research Centres to Develop Privacy-Preserving Tech and Train Talent, Government & Economy. *The Business Times*, January 18. <https://www.businesstimes.com.sg/government-economy/two-new-research-centres-to-develop-privacy-preserving-tech-and-train-talent>.
- Singapore Academy of Law, Law Reform Committee, & Constantine, S. 2020. Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars, Singapore. [https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020\\_Report%20on%20the%20Attribution%20of%20Civil%20Liability%20for%20Accidents%20Involving%20Autonomous%20Cars.pdf](https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020_Report%20on%20the%20Attribution%20of%20Civil%20Liability%20for%20Accidents%20Involving%20Autonomous%20Cars.pdf)
- Singapore Public Service. 2020. “Instruction Manual: Government Data Architecture.” <https://www.psd.gov.sg/challenge/ideas/work-better/instruction-manual-government-data-architecture>.
- Singapore Statutes Online. 2022. “Road Traffic Act 1961—Singapore Statutes Online.” <https://sso.agc.gov.sg:5443/act/rta1961>.
- Smart Nation and Digital Government Office. 2022. “Our Achievements. Singapore Topped the IMTD-SUTD Smart City Index for 3rd Year Running.” March 9. <https://www.smartnation.gov.sg/about-smart-nation/our-journey/achievements>.
- Smart Nation Singapore. 2018. “Digital Government Blueprint “A Singapore Government that is Digital to the Core, and Serves With Heart.” <https://www.smartnation.gov.sg/files/publications/dgb-booklet-june2018.pdf>.
- Smart Nation Singapore. 2020. “Digital Government Blueprint “A Singapore Government That is Digital to the Core, and Serves with Heart.” [https://www.tech.gov.sg/files/media/corporate-publications/dgb-public-document\\_30dec20.pdf](https://www.tech.gov.sg/files/media/corporate-publications/dgb-public-document_30dec20.pdf)
- Smart Nation Singapore. 2022. “Pillars of a Smart Nation.” August 24. <https://www.smartnation.gov.sg/about-smart-nation/pillars-of-smart-nation>.
- Spichkova, M., and M. Simic. 2015. “Towards Formal Modelling of Autonomous Systems.” In: Damiani, E., Howlett, R., Jain, L., Gallo, L., De Pietro, G. (eds) *Intelligent Interactive Multimedia Systems and Services. Smart Innovation, Systems and Technologies*, vol 40., 279–288, Springer, Cham. 10.1007/978-3-319-19830-9\_25
- SS ISO 10218-2. 2016. *Robots and robotics devices—Safety requirements for industrial robots Part 2: Robot systems and integration* [Singapore Standard]. Singapore Standards Council, Enterprise Singapore, Singapore.
- SS ISO 13482. 2017. *Robots and Robotics Devices—Safety Requirements for Personal Care Robots* [Singapore Standard]. Singapore Standards Council, Enterprise Singapore, Singapore.



- Such, J. M. 2017. Privacy and Autonomous Systems, In Proceedings of the 26th International Joint Conference on Artificial Intelligence (IJCAI'17). AAAI Press, 4761–4767. Melbourne, Australia, August 19 - 25, 2017.
- Tan, S. Y., and A. TAEIHAGH. 2020. “Smart City Governance in Developing Countries: A Systematic Literature Review.” *Sustainability* 12 (3): 899. doi:10.3390/su12030899.
- Tan, S. Y., and A. TAEIHAGH. 2021. “Adaptive Governance of Autonomous Vehicles: Accelerating the Adoption of Disruptive Technologies in Singapore.” *Government Information Quarterly* 38 (2): 101546. doi:10.1016/j.giq.2020.101546.
- Tay, S. 2020. “The Secret to Singapore’s Data-Driven Government.” GovInsider, December 3. <https://govinsider.asia/data-and-transformation/the-secret-to-singapores-data-driven-government/>.
- TR 108: 2022. 2022. *Safe Deployment of Robots on Healthcare Sector* [Technical Reference]. Singapore Standards Council, Enterprise Singapore, Singapore
- TR 93: 2021. 2021. *Data Exchange Between Robots, Lifts and Automated Doorways to Enable Autonomous Operations* [Technical Reference]. Singapore Standards Council, Enterprise Singapore, Singapore.
- Uckelmann, D., M. Harrison, and F. Michahelles. 2011. “An Architectural Approach towards the Future Internet of Things.” In *Architecting the Internet of Things*, 1–24. Springer, Berlin, Heidelberg.
- United Nations. 2018. “68% Of the World Population Projected to Live in Urban Areas by 2050, Says UN | UN DESA | United Nations Department of Economic and Social Affairs.” May 16. <https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html>
- Van Panhuis, W. G., P. Paul, C. Emerson, J. Grefenstette, R. Wilder, A. J. Herbst, D. Heymann, and D. S. Burke. 2014. “A Systematic Review of Barriers to Data Sharing in Public Health.” *BMC Public Health* 14 (1): 1–9. doi:10.1186/1471-2458-14-1144.
- Viberg Johansson, J., H. B. Bentzen, and D. Mascalzoni. 2022. “What Ethical Approaches Are Used by Scientists When Sharing Health Data? An Interview Study.” *BMC Medical Ethics* 23 (1): 1–12. doi:10.1186/s12910-022-00779-8.
- Wang, J., E. Schluntz, B. Otis, and T. Deyle. 2015. A New Vision for Smart Objects and the Internet of Things: Mobile Robots and Long-Range UHF RFID Sensor Tags. ArXiv Preprint ArXiv:1507.02373. <https://doi.org/10.48550/arXiv.1507.02373>
- Watson, D. P., and D. H. Scheidt. 2005. “Autonomous Systems.” *Johns Hopkins APL Technical Digest* 26 (4): 368–376.
- Yin, R. K. 2017. *Case Study Research and Applications: Design and Methods*. Sage publications: Los Angeles.
- Zanussi, Z. 2021. “A Brief Survey of Privacy Preserving Technologies.” <https://www.statcan.gc.ca/en/data-science/network/privacy-preserving>
- Zhang, K., J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen. 2017. “Security and Privacy in Smart City Applications: Challenges and Solutions.” *IEEE Communications Magazine* 55 (1): 122–129. doi:10.1109/MCOM.2017.1600267CM.