PRIVACY

4. PRIVACY

The City of Toronto will support and enhance data privacy as it relates to the collection and use of information generated by automated vehicles.

Privacy plays a key role in a free, democratic society and is an essential element in maintaining public trust in government. The City of Toronto is committed to protecting the privacy of individuals and will ensure that privacy protection continues to play a key role in an open, accessible and transparent government.

With the introduction of AVs, the volume and variety of data generated and transmitted between vehicles, infrastructure, connected devices, and third party data repositories will increase substantially.[49] However, realizing some of the potential benefits to traffic management, traveller information, safety, enforcement and more – is dependent on establishing stringent standards and clear guidelines around the privacy of these vehicles.[50]

The City of Toronto is subject to the Province of Ontario's Municipal Freedom of Information and Protection of Privacy Act, which provides a right of access to City information while at the same time protecting the privacy of individuals.[51] However, contemporary issues of data governance still need to be resolved and standards must be in place to protect the data of individuals using AVs and the general public outside the vehicle.

In addition to legislative requirements to ensure privacy, Privacy by Design guidelines provide a strong foundation, requiring AV technology developers to take proactive steps to ensure users' privacy is minimally invaded.[52]

The future of urban, data-driven mobility depends on government, private mobility companies, and the public having confidence that their data is being used in the way it is intended.

GUIDING POLICIES AND STRATEGIES:

The City of Toronto's Protection of Privacy Policy:
The City of Toronto will:

a. *Ensure all employees share responsibility for the protection of personal information privacy and compliance with the roles and responsibilities identified in this Policy;*
b. *Plan for and ensure that privacy protection requirements are embedded in the design of all City programs, processes, projects and technology architecture.*
c. *Establish and communicate a set of privacy standards and guidelines to improve the protection of personal information by identifying, investigating, assessing, monitoring and mitigating personal information privacy risks in City programs and activities involving the collection, use, disclosure and disposal of personal information.*
d. *Apply this policy and related policies and practices in the collection, use, disclosure, and disposal of personal information;*
e. *Clearly communicate to the public how personal information is collected, used, disclosed and disposed.*

4. PRIVACY

4.1 Protect Public Privacy

Key Performance Indicators

- Month-over-month percentage +/- (increase/decrease) of privacy breaches that result in unauthorized data discovery, and leakage, of personal information

Tactics

4.1.1 Data Privacy Standards
4.1.2 Privacy Standards: Automated Transit Vehicles
4.1.3 Privacy Standards: Shared AV Fleets
4.1.4 Privacy Governance and Oversight
4.1.5 Privacy Principles: Privacy by Default
4.1.6 Privacy Attestation Services

4. PRIVACY

4.1 PROTECT PUBLIC PRIVACY

In 2050, the City will have ensured that a robust mechanism for the governance of data generated by driving automation systems is in place prior to the widespread adoption of automated vehicles. This is to protect the privacy of transportation system users and their data.

4.1.1 Data Privacy Standards

Proposed Tactic: Develop and implement a policy and mechanisms consistent with Privacy by Design principles, to address ownership, custody, usage, and safeguarding of data associated with a natural person.

AVs will create new real-time data connections between vehicles, infrastructure, connected devices, and third-party data repositories. In order for a data-driven mobility system to work, government, private transportation companies, and the public need to be confident that their privacy is being protected and their data is being used in a way to which they have they have given their informed consent.

Additionally, Toronto's residents should be able to quickly understand how these technologies work and the purposes they serve. One way this could be accomplished is through signage that highlights what type of data is being collected in and around the vehicle and how it will be used.[53]

To the greatest possible extent, the City will advocate for the adoption of Privacy by Design principles in the automated vehicle environment prior to the widespread introduction of AVs. This means addressing privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data by practicing the following seven Foundational Principles:[52]

Principle 1: Proactive not reactive: preventative not remedial
Principle 2: Privacy as the default setting
Principle 3: Privacy embedded into design
Principle 4: Full functionality: positive-sum, not zero-sum
Principle 5: End-to-end security: full lifecycle protection
Principle 6: Visibility and transparency: Keep it open
Principle 7: Respect for user privacy: Keep it user centric

Furthermore, the City will participate in the development of federal privacy standards and, where required, create policies and standards that address AVs.

- *Proposed progress to 2022: The City will develop a policy framework to address privacy aspects as it relates to the ownership, custody and usage of personally identifiable data captured from AVs, as well as corporate procurement standards.*

4.1.2 Privacy Standards: Automated Transit Vehicles

Proposed Tactic: Develop and implement policies to ensure automated transit vehicle riders understand what personal data is accessed and collected from them.

4. PRIVACY

TTC vehicles today are equipped with video cameras to ensure the safety and security of employees, customers and property. Smart fare collection systems record the time and location of trips and are often linked to customer profiles.

Recognizing the need to minimize privacy intrusion, TTC currently does not allow any unauthorized copies of data/images in any format (hardcopy, electronic, etc.) to be taken from the video recording system.

TTC will take all possible measures to ensure that if connected technologies (e.g., V2X) are introduced into transit vehicles, personally identifiable information is not accessible to malicious agents over the air.

- *Proposed progress to 2022: Research and learn more about the privacy impacts for automated transit vehicles.*

4.1.3 Privacy Standards: Shared AV Fleets

Proposed Tactic: Develop and implement policies to ensure shared AV fleet service consumers are educated about what personal data is accessed and collected from them.

The primary method of matching ride hailers to ride providers for shared fleet companies currently is through the collection, retention and processing of personal and public data on their users. This information includes home address, contact information, payment details, device locations, trip histories, and more.[54][55]

As automation increases the amount of data that can be collected, privacy concerns also increase.[56] Data will permeate most aspects of the AV experience and companies are likely to want to monetize this data as an additional revenue stream. The City of Toronto has a responsibility to ensure that, to the greatest extent possible, any personally identifiable information is de-identified at the source, and the public is aware of what data is being gathered and used when they take a ride in a shared fleet AV.

- *Proposed progress to 2022: Research and learn more about the privacy impacts for shared AV fleet consumers.*

4.1.4 Privacy Governance and Oversight

Proposed Tactic: Develop and implement an enterprise automated vehicle assurance framework that reflects the City's authority over, and oversight of, data privacy protection across multiple dimensions/domains.

An enterprise AV assurance framework will ensure that the data privacy, and protection, aspects of this technology, including threats to the enterprise itself are addressed through an overarching, programmatic approach.

An enterprise consists of the people, processes, environment and automated information systems associated with AVs and to have a successful assurance framework for this, the capability to withstand attack should be true across all components.[57]

4. PRIVACY

▶ *Proposed progress to 2022: Develop an AV enterprise assurance framework for the City to implement as it relates to their authority over, and oversight of data privacy protection.*

4.1.5 Privacy Principles: Privacy by Default

Proposed Tactic: Support the development and adoption and adoption of automated vehicle technology consistent with Privacy by Default principles.

Individuals signing up for online and connected services (e.g., social media) may unknowingly be sharing personally identifiable information, without having explicitly opting to do so. As more vehicles become connected through navigation apps, infotainment systems and other software, the risk of users unknowingly broadcasting their personally-identifiable information could increase significantly.

The Privacy by Default principle – one of the seven Privacy by Design foundational principles – states that when a system or service includes choices for the individual on how much personal data they share with others, the default settings should be the most privacy-friendly ones.[58] This consists of several components:[59]

- Privacy controls should default to the protected state rather than having to be activated or selected (i.e. controls are built in and automatically switched on).
- The collection of personal information is limited to that necessary for the primary purpose identified in the notice
- Personal information is used only for the primary purpose(s) identified and only if the individual has provided implicit or explicit consent, unless a law or regulation specifically requires otherwise.

▶ *Proposed progress to 2022: Design and develop a mechanism that will determine if and how Privacy by Default principles are embedded into AV technology.*

4.1.6 Privacy Attestation Services

Proposed Tactic: Develop and implement a standard for the City through which the accuracy of AV data privacy protections can be verified.

AVs along with their supporting technologies, bring with them increased capabilities and demand for interconnectedness, data analytics and sharing of information to deliver a better customer experience as well as increased use of cloud computing and mobile devices.[60]

However, this brings risks: privacy breaches are becoming more common, whether due to human error, employee indiscretion or cyber-attacks. This has led to heightened compliance obligations, increased regulatory enforcement, and increased privacy awareness and expectations from the public.

To address these challenges, the City will adopt a Privacy by Design certification and accreditation process which would assess AV products, services, processes or systems against the privacy by design principles and related privacy control framework (e.g., through a risk scorecard technique). By doing so, it would ensure privacy and security—through every phase of the data lifecycle (e.g. collection, use, retention, storage, disposal or destruction) — the key benefits of which are to fostering greater public trust by demonstrating residents' data is secure and privacy is being well managed and continuously updated.

▶ *Proposed progress to 2022: Develop a minimum data privacy protection standard for the City to undertake.*