PRELIMINARY REPORT #2 FROM BATCH 5 OF THE IOT STANDARDS DEVELOPMENT PROJECT

CONTRIBUTIONS TO A CONCEPTUAL FRAMEWORK FOR MANAGING THE SOCIAL AND ETHICAL ISSUES OF URBAN IOT

FEBRUARY 2018

Prepared for:

Ville de Montréal

For: Mr. Jean-Martin Thibault

Director (CTO), IT Architecture, Innovation and Security

Ville de Montréal

275, rue Notre-Dame Est

Montréal, QC, HCY 1C6

Canada

POLYTECHNIQUE MONTRÉAL

This report was prepared by CIRAIG (Centre international de reference sur le cycle de vie des produits procédés et services).

CIRAIG was established in 2001 to provide businesses and government with academic, state-of-the-art expertise on sustainable development tools. CIRAIG is one of the world's leading centres of life cycle expertise. The organization works with many research centres throughout the world and actively participates in the life cycle initiative of the United Nations Environment Programme (UNEP) and the Society of Environmental Toxicology and Chemistry (SETAC).

CIRAIG has developed recognized expertise in life cycles tools, including environmental life cycle assessment (ELCA) and social life cycle assessment (SLCA). Its research complements this expertise, with studies on life cycle cost analyses (LCCAs) and other tools, including carbon and water footprints. CIRAIG's activities include applied research in many critical sectors, such as energy, aerospace, agrifood, waste management, pulp and paper, mines and metals, chemical products, telecommunications, finance, urban infrastructure management, transportation and green product design.

CIRAIG
Centre international de reference sur le cycle
de vie des products, procédés et services
Polytechnique Montréal
Département de génie chimique
3333, chemin Queen-Mary, suite 310
Montréal (Québec) Canada
H3V 1A2
www.ciraig.org

Research Team

Research Team

Execution

Sara Russo Garrido

Supervision, Research and writing

Marie-Luc Arpin

Revision

Project Management

Prof. Nicolas Merveille PhD

Professor, ESG UQAM and CIRAIG

Project Participants from the Ville de Montréal:

Jean-Martin Thibault, Pierre-Antoine Ferron, Stéphane Guidoin, Michel Charest, Song Nhi Nguyen, Martin-Guy Richard and Patrick Lozeau.

Summary

Project Mission

This report seeks to lay a to guide Montréal in developing for defining a conceptual framework that can guide Montréal in establishing a program for considering and managing issues of ethics and social acceptability associated with the technological and analytical systems of an urban Internet of things. These systems are responsible for collecting data from many sources (municipal sensors, social networks, external databases), internal processing, storage and analysis of such data, as well as for releasing this data in the form of databases, displays or apps for the public. This report builds on *the Literature Review: Ethical Issues and Social Acceptability of IoT in the Smart City*[1] (Russo Garrido, et al., 2017).

The report presents two frameworks to guide Montréal in developing one or more conceptual frameworks for ethical governance of IoT:

- Framework to assist in the identification and analysis of issues of ethics and social acceptability in IoT.
- A list of principles to guide how these issues are handled.

These elements do not, on their own, constitute a comprehensive conceptual framework. However, they are important milestones in the development of a more complete and scalable framework.

Frameworks for Identifying Ethical and Social Issues

Frameworks for identifying the ethical and social issues discussed in this report are designed to provide decision-makers with tools that will help them identify and study issues associated with the IoT project. These frameworks are based on the following sources of information, with most taken from the literature review (Russo Garrido, et al., 2017):

- Key components of the IoT system, as operated by the city.
- Ethical issues identified in the literature review or in the opinion of the Commission d'éthique en sciences et technologie du Québec sur les villes intelligentes (CÉSTQ, 2017).

The broad outlines of the IoT are described in the following figure.

[1] The Complete Title Is: *Final Report #1 For Batch 5 of the IoT Standards Development Project Literature Review: Ethical Issues and Social Acceptability of IoT in the Smart City*.

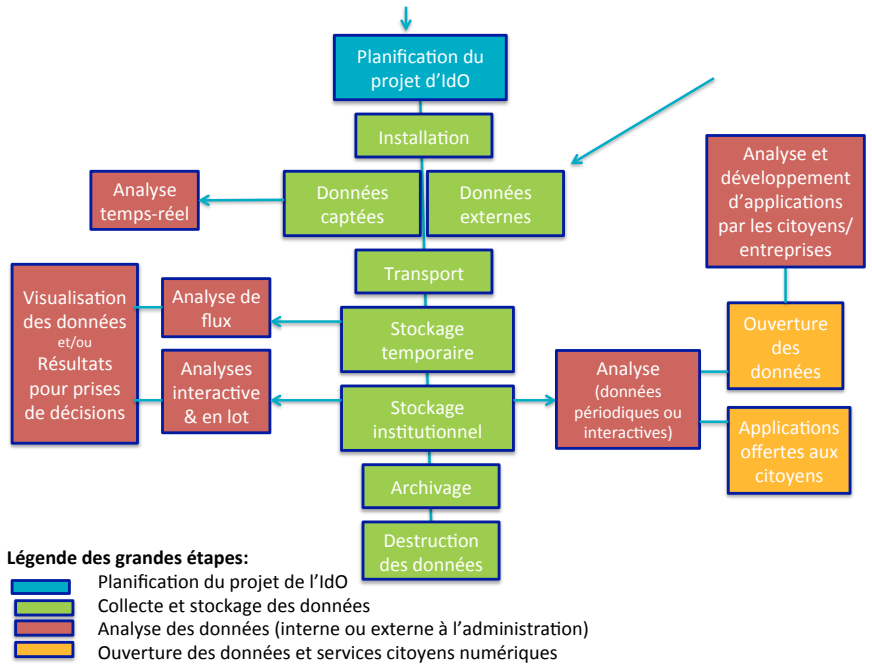


Figure A: Components of Montréal's IoT System

As explained in the literature review, the system can be broken down into four main phases:

- IoT project planning.
- Data collection and storage.
- Data analysis (internal or outside the city)
- Open data and digital services for the public.

Based on these steps and the ethical and social issues identified in the literature review and the CÉSTQ (2017) opinion, we propose the following framework for high-level identification of ethical issues.

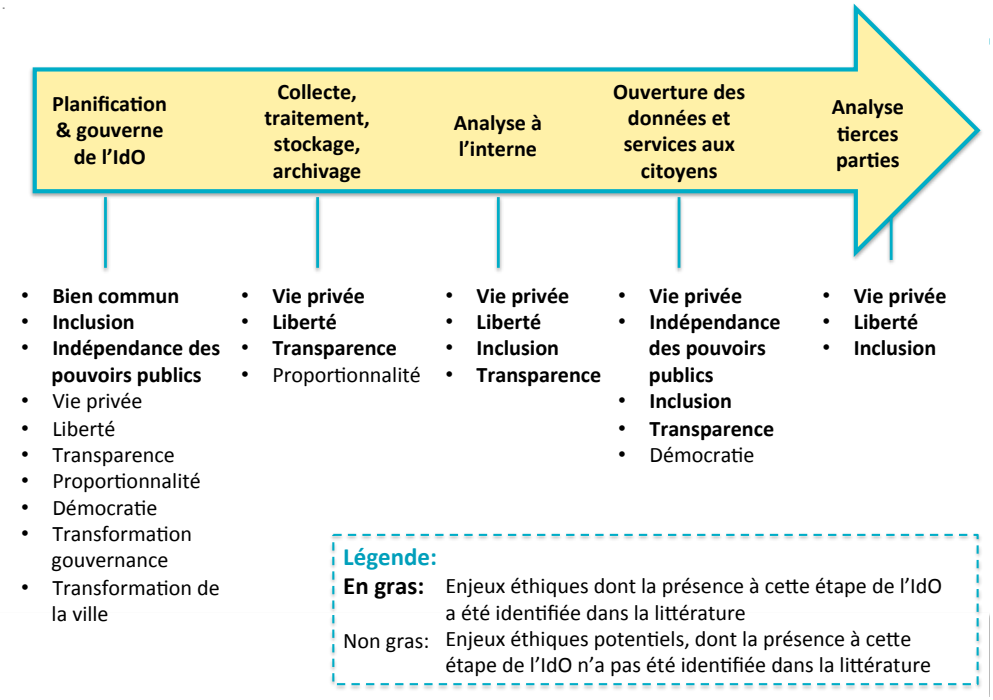


Figure B: General Framework for High-Level Identification of Issues of Ethics and Social Acceptability

While the framework outlined below may be useful for general discussion, more specific frameworks are needed that not only identify general concerns, but provide a more detailed definition of activities and situations that could give rise ethical or social issues. Figures C, D and E present this level of detail, each illustrating a set of issues covered in the literature review (as indicated by each figure's title).

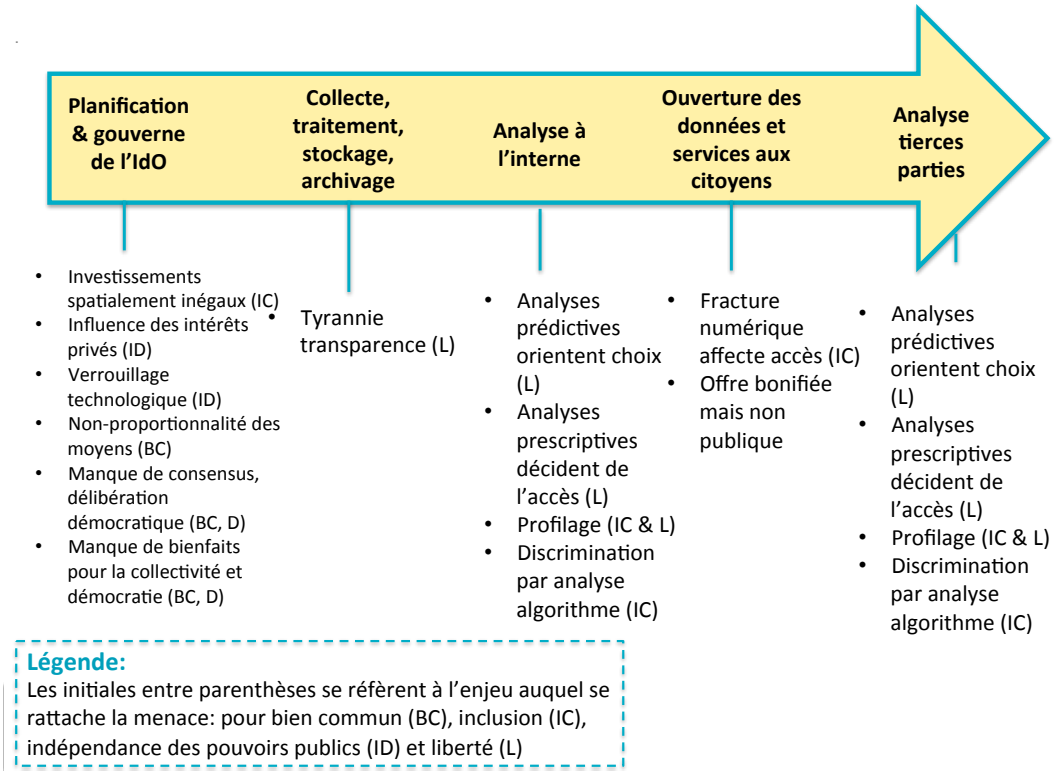


Figure C: Threats Pertaining to Issues of the Public Good, Social Inclusion, Separation of the Government and Business Spheres, and Freedom

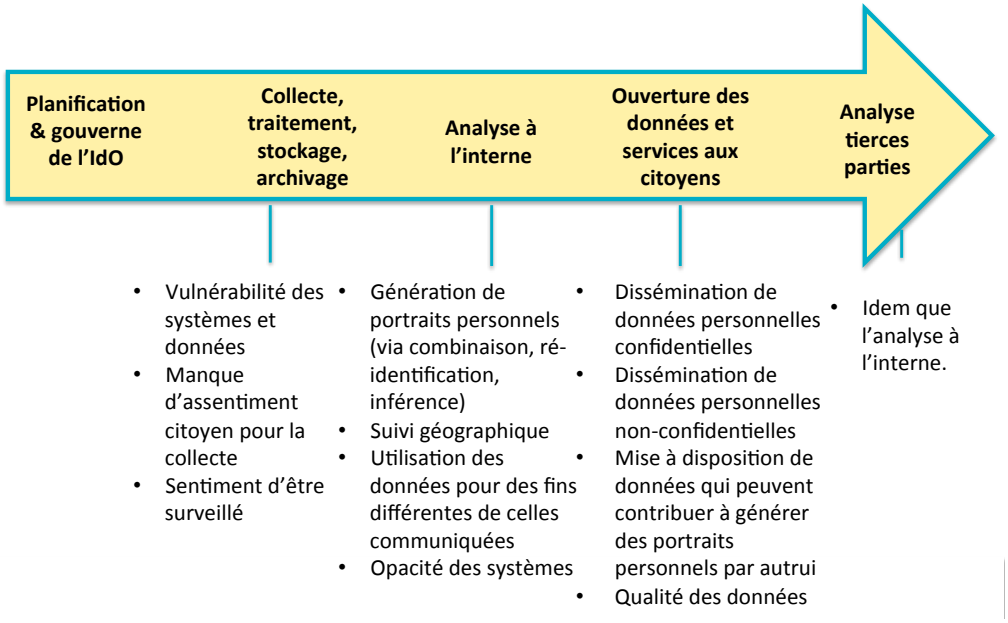


Figure D: Threats Pertaining to Privacy and Transparency

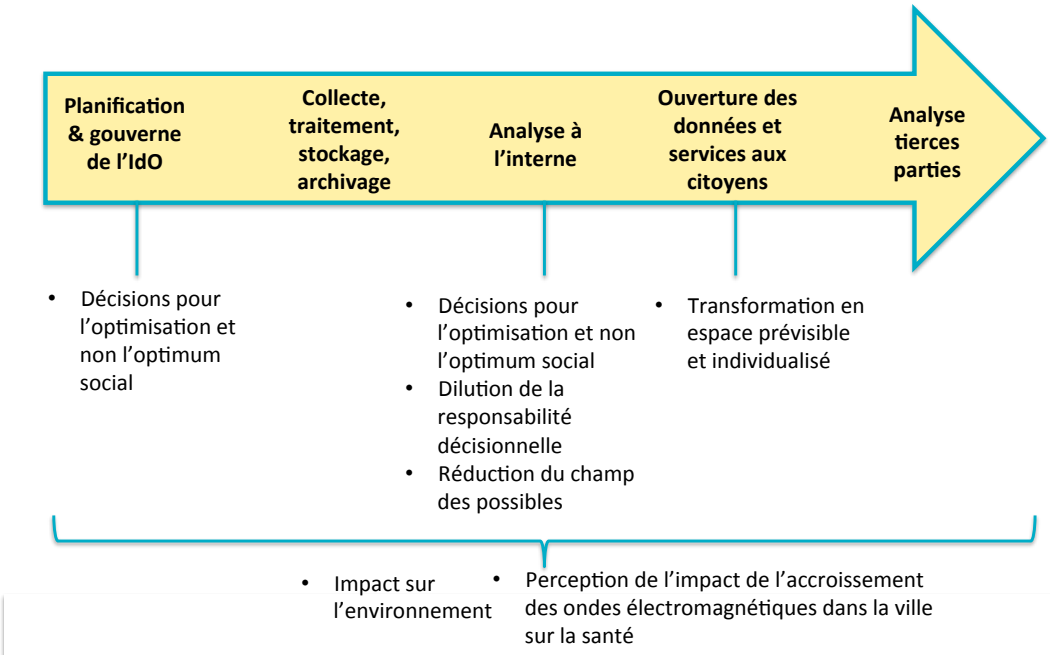


Figure E: Threats Pertaining to Transformation of Governance and the City

Issue Analysis and Management Principles

The second contribution of this report is a list of principles to apply in examining and managing issues. This list is designed to incorporate the key principles for addressing issues of ethics and social acceptability arising out of IoT. It is intended to help determine the appropriate approach in an environment characterized by change, innovation, transformation of the social bond and a loss of ethical references.

We decided to build on all relevant existing guidelines on the subject, in developing this list, rather than start from scratch. We have accordingly considered the principles proposed for IoT, the smart city, artificial intelligence and big data research. The following box outlines our procedure:

Procedure for Developing the List of Principles

1. Create an inventory of existing relevant principles.
2. Extract and examine all principles, to understand their characteristics and see how they overlap.
3. Develop a final list of principles pertaining to IoT and the completeness with respect to other lists consulted.
4. Consider overlaps between the proposed list of principles and the literature review's findings.
5. Identify principles that should be enhanced and subsequent steps.

We selected lists of existing principles based on their relevance and importance. The following table identifies these documents, grouped by their technological or thematic focus. Section 3.3 presents these lists in detail.

Table A: Lists of Principles Considered

Category	Lists of Principles
General privacy principles	• Canadian PIPEDA fair information principles • Fair Information Practice Principles (FIPPs) • OECD Guidelines • Privacy by Design • Information and Privacy Commissioner of 7 Foundational Principles of Privacy by Design • City of Seattle Privacy Principles • EU general legislation of 1990 and 2018
General IoT and smart city principles	• Recommendations on smart cities in the Opinion of Québec's Commission en éthique sciences et technologie • NYC's Guidelines for Building a Smart + Equitable City
Artificial intelligence principles[2]	• Asilomar AI Principles • Fair Automation Practice Principles (FAPPs) • The Montreal Declaration for a Responsible Development of Artificial Intelligence
Big data principles[3]	• Ten simple rules for responsible big data research
Codes of conduct	• ACM Code of Ethics and Professional Conduct • IEEE Code of Conduct[4]

We drew up a final list of principles, drawing on the 13 documents appearing in Table A. These principles were then classified, summarized and distilled to produce a final list, in line with the following criteria:

[2] The IEEE's deliberations (IEEE, 2017) on artificial intelligence can be added to this list for subsequent contributions to the inventory.

[3] The principles presented in the article by Richards and King (2014) could be added here for subsequent contributions to the inventory.

[4] ACM and IEEE jointly produced a code, but we did not cover it in this study. Since IEEE is in the process of creating a new version of its own code, we decided to stick to the latest codes, rather than those produced as part of a collaborative process.

- Comprehensiveness: maximum coverage of topics identified in the lists of principles consulted.
- Relevance: all topics directly pertain to the management of ethical issues and the various technical components of the IoT system.[5]
- From the general to the specific: identification of a limited number of general principles and dividing them into more specific ones.

Obviously, our proposed framework is a starting point. It must evolve and become more robust through consultation and verification of other reference documents, deliberations within the city and broader consultations with stakeholders.

The following table presents the 11 key principles proposed. They can then be broken into subprinciples or specific principles as presented in Appendix G.[6] Determining the final principles and desired levels of specificity is up to the city.

[5] However, the study did not cover principles on overall good IoT governance (in terms of infrastructure maintenance, efficiency, etc.).

[6] Appendix G also transparently describes the sources of the key principles proposed (the list, framework or code from which they were taken), as well of lists of principles that overlap in certain areas.

Table B: List of Proposed Principles

Thème	Principe
Bien commun	Assurer que l'IdO soit au service du bien commun et de la recherche d'un optimum social.
Démocratie et participation citoyenne	Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique
Vie privée	Protéger et respecter la vie privée* des citoyens
Transparence	Être transparent sur le « qui, quoi, quand, où, pourquoi et comment » de la collecte, la transmission, le traitement et l'utilisation
Sécurité	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Bonne gestion des données	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Évaluations et conséquences	Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données et veiller à l'analyse des conséquences à long terme sur les valeurs sociales élargies
Équité et inclusion	Mettre tous les moyens en œuvre pour que le traitement accordé tous soit juste et impartial. Éviter le profilage, la discrimination et le renforcement des inégalités pour développer un projet inclusif
Autonomie des pouvoirs publics	Assurer l'autonomie de la sphère publique et la primauté de l'intérêt public par rapport aux intérêts privés
Systèmes explicables	Concevoir des systèmes auditables et dans des cas de prise de décision automatisée, donner aux individus accès aux logiques qui président dans la décision, ainsi qu'une explication des données utilisées (quelle donnée, quelle source, comment est-elle mobilisée)
Liberté	Assurer que le citoyen puisse préserver son sentiment de liberté

*There has been much debate over defining privacy. In this report, the term refers to personal freedom against any physical intrusion, any interference in personal life and any impediment to a person's ability to control the access and use of their personal information.

Generally, the issues and threats documented in the literature review (as appear in Figures C, D and E) are relatively well covered by the list of principles proposed. Just the issues of "freedom" and "transformation of the city" receive only partial treatment by this framework, to which we have added general or specific principles (to be defined) to ensure complete coverage, as explained in Section 4.1.

Next Steps

While the list of proposed principles is the fruit of a meticulous effort to amass existing best practices for dealing with the ethical and social issues of an IoT system, as planned for Montréal, there are several steps involved in perfecting this list and making it fully useful. Section 4.2 presents subsequent steps recommended for future enhancement of the list, including: 1) Debating, reformulating as required, selecting and validating the 10 proposed principles and their specific related principles within and without city government. 2) Identifying any missing specific principles. 3) As discussed in Section 4.1., reinforcing weak specific principles. 4) Identifying how the framework defines specific practices at each stage of the IoT system. In other words, we must be able to express the stated principles as specific practices applicable to the daily routines of city officials.

Conclusion

This report presents frameworks designed to guide Montréal in developing one or more conceptual frameworks for ethical governance of IoT. As previously mentioned, these elements do not on their own constitute complete conceptual frameworks. However, they are important milestones in developing a more complete framework. To date, these elements can make significant contributions to the deployment of optimal analytical and management practices, and taking action on issues of ethics and social acceptability with respect to Montréal's IoT system. In other words, we can only deal with the uncertainty and changes due to the deployment in the city of new technologies by adopting tools to support an ongoing watch of emerging issues and develop corresponding practices that will contribute to the dialogue on the next steps to take and society's choices in the matter.

Contents

Tables

Figures

Abbreviations and Acronyms

ACM	Association of Computing and Machinery
CÉSTQ	Commission d'éthique en sciences et technologies du Québec
FAPPs	Fair Automation Practice Principles
FIPPs	Fair Information Practice Principles
AI	Artificial intelligence
IoT	Internet of Things
IEEE	Institute of Electrical and Electronics Engineers
NYC	New York City
OECD	Organisation for Economic Cooperation and Development

1 Introduction

This report seeks to lay a to guide Montréal in developing for defining a conceptual framework that can guide Montréal in establishing a program for considering and managing issues of ethics and social acceptability associated with the technological and analytical systems of an urban Internet of things. These systems are responsible for collecting data from many sources (municipal sensors, social networks, external databases), internal processing, storage and analysis of such data, as well as for releasing this data in the form of databases, displays or apps for the public.

The report builds on the *Literature Review: Ethical Issues and Social Acceptability of IoT in the Smart City*[7] (Russo Garrido, et al., 2017), which identified the most likely issues for the city, based on numerous studies and the prior experiences of municipalities around the world. It seeks to guide Montréal's deliberations on developing one or more conceptual frameworks for ethical governance of IoT and proposes two frameworks to drive this process:

- Framework to assist in the identification and analysis of issues of ethics and social acceptability in IoT.
- A list of principles to guide how these issues are handled/.

These elements do not, on their own, constitute a complete conceptual framework. However, they are important milestones in the development of a more complete and scalable framework.

Section 2 of this report initially focuses on the first issue identification framework, largely based on the above-mentioned literature review. Section 3 describes the process used in developing a list of principles. Section 4 presents this list. The Conclusion summarizes what has been done so far and the next steps to take.

[7] The Complete Title Is: *Final Report #1 For Batch 5 of the IoT Standards Development Project Literature Review: Ethical Issues and Social Acceptability of IoT in the Smart City*.

2 Issue-Identification Framework

Our framework for identifying ethical and social issues is designed to provide decision-makers with a tool that can help them identify and study issues associated with the IoT project. This framework is based on two core elements:

- Key components of the IoT system, as operated by the city.
- Ethical issues identified in the literature review and in the opinion of the Commission d'éthique en sciences et technologie du Québec sur les villes intelligentes (CÉSTQ, 2017).

In short, this framework is based on the conclusions of the literature review that constitutes the first part of this project, adding some new ideas taken from CÉSTQ's opinion (2017). While the framework contains no original research, its presents a new structure for the information appearing in the first report under this project.

2.1 Key Components of the IoT System

As mentioned in the Introduction, IoT systems are responsible for collecting data from many sources (municipal sensors, social networks, external databases), internal processing, storage and analysis of such data, as well as for releasing this data in the form of databases, displays or apps for the public. The following figure presents a simplified view of Montréal's IoT system:

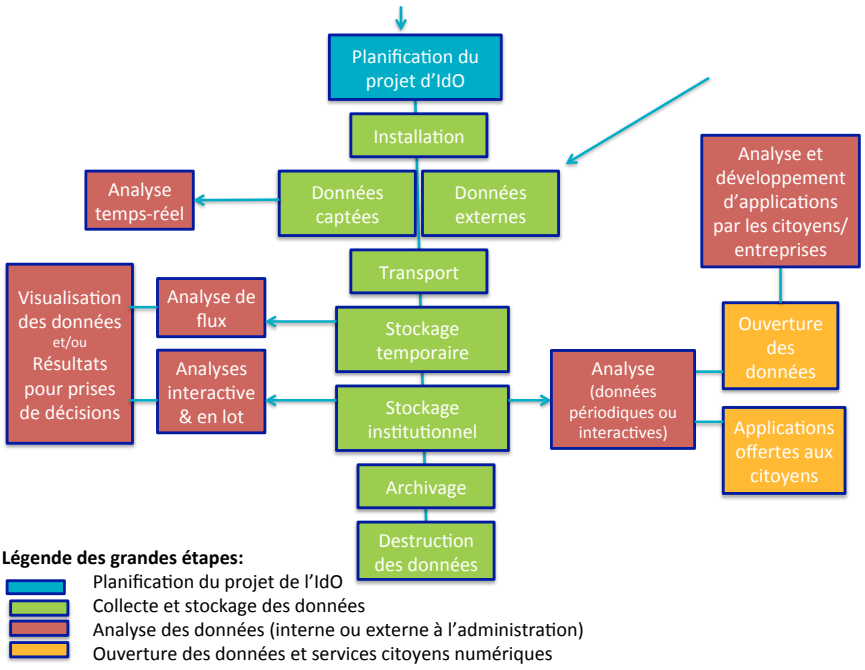


Figure 1: Components of Montréal's IoT system

As explained in the literature review, the system can be broken down into the four main phases of system activities:

- IoT project planning.
- Data collection and storage.
- Data analysis (internal or outside the city)
- Open data and digital services for the public.

2.2 Issues Identified in the Literature Review

Figures 2, 3 and 4 summarize potential issues of ethics or social acceptability that are identified in the literature. These issues are grouped by the major IoT system phase in which they occur. Phase-specific threats that give rise to such these ethical issues are also indicated, as found in the literature.

Figure 4 also highlights IoT-related ethical issues named in the opinion on smart cities issued by the Commission d'éthique en sciences et technologies du Québec (CÉSTQ, 2017). The figure does not include all elements identified by the CÉSTQ, but only those *that pertain to* IoT and *complement* the issues identified in the literature review.

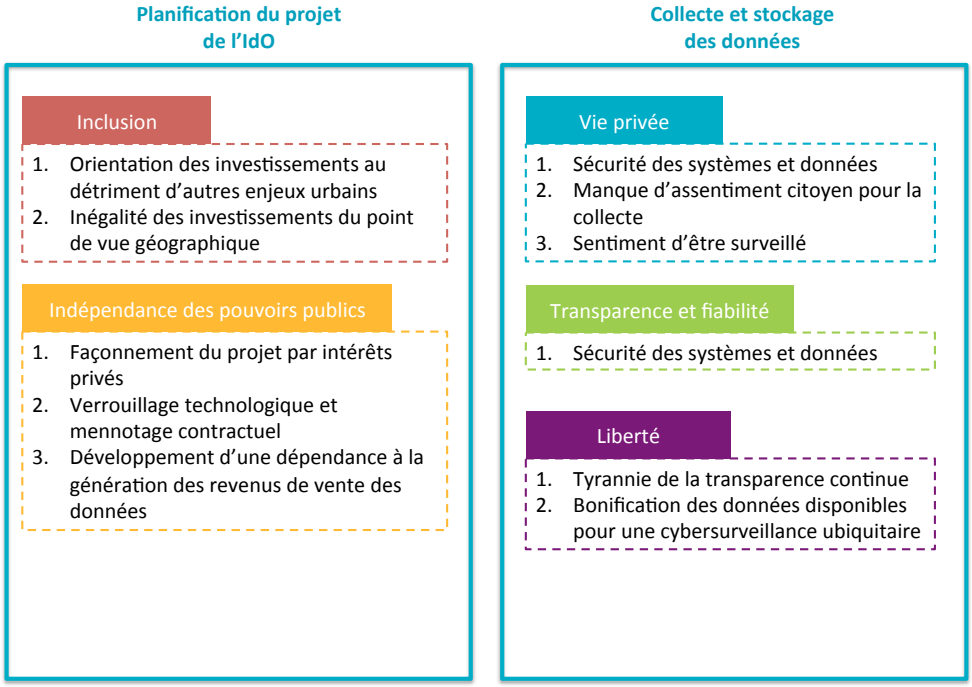


Figure 2: Ethical Issues and Related Threats in the Planning and Data Collection/Storage Phases

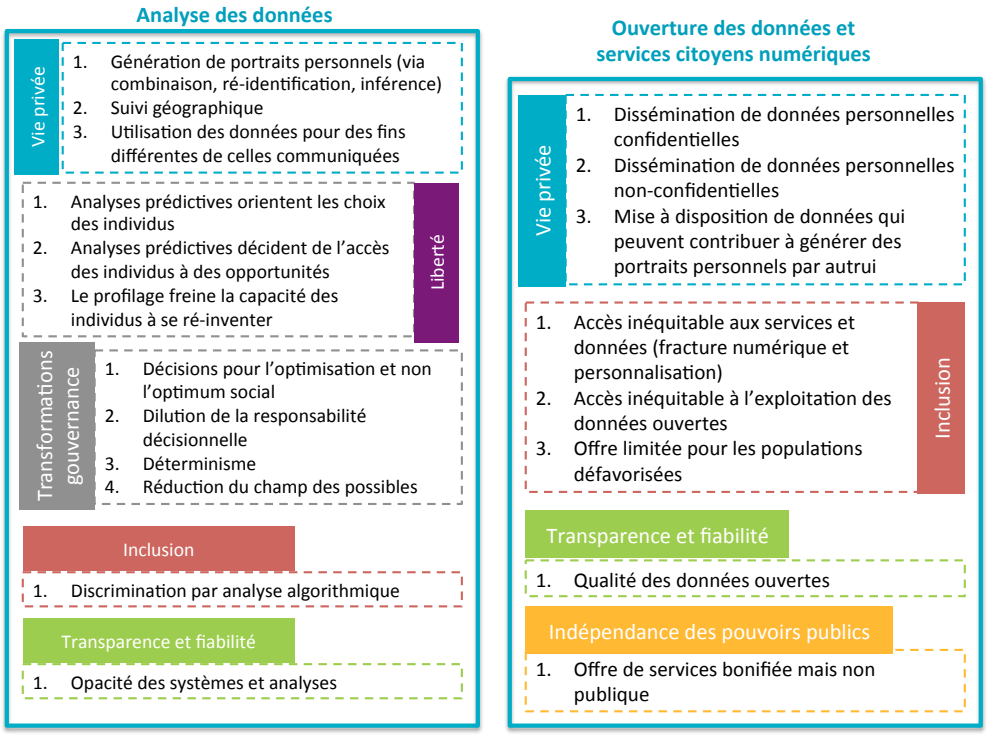


Figure 3: Ethical Issues and Related Threats at the Data Analysis and Release Phases

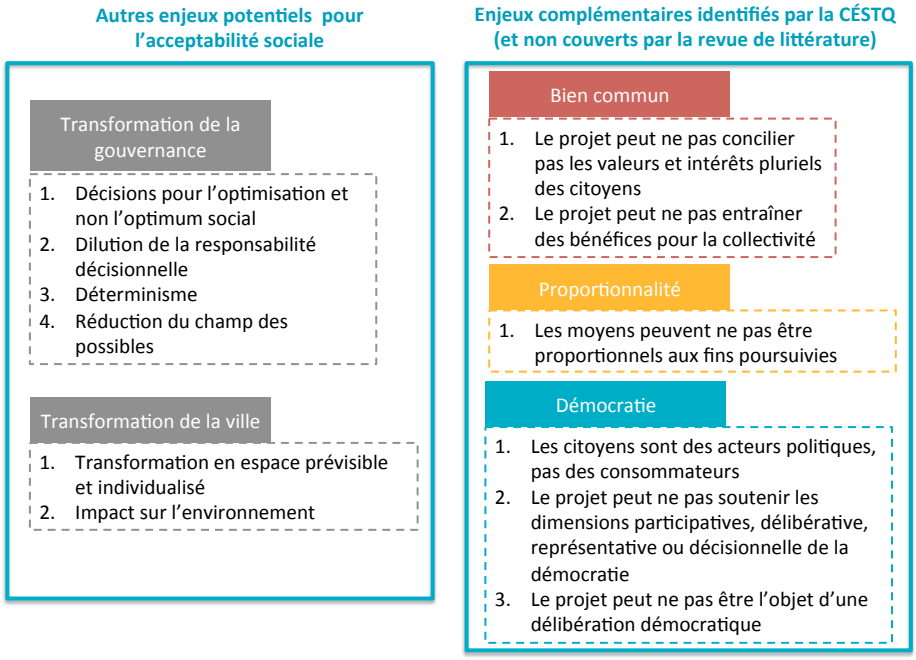


Figure 4: Other Issues Pertaining to Social Acceptability and the CÉSTQ's Opinion

2.3 Proposed Issue Identification Support Framework

Based on the IoT system's main components, the ethical and social issues identified in the literature review, and the opinion of the Commission d'éthique en sciences et technologie du Québec, we propose the following framework for high-level identification of ethical issues. As appears in the legend, issues corresponding with a particular IoT phase (planning, analysis, etc.) and appearing in bold characters are ethical ones identified in the literature. Non-bolded items at the IoT phase are potential issues that have been not been identified in the literature, but could still be present.

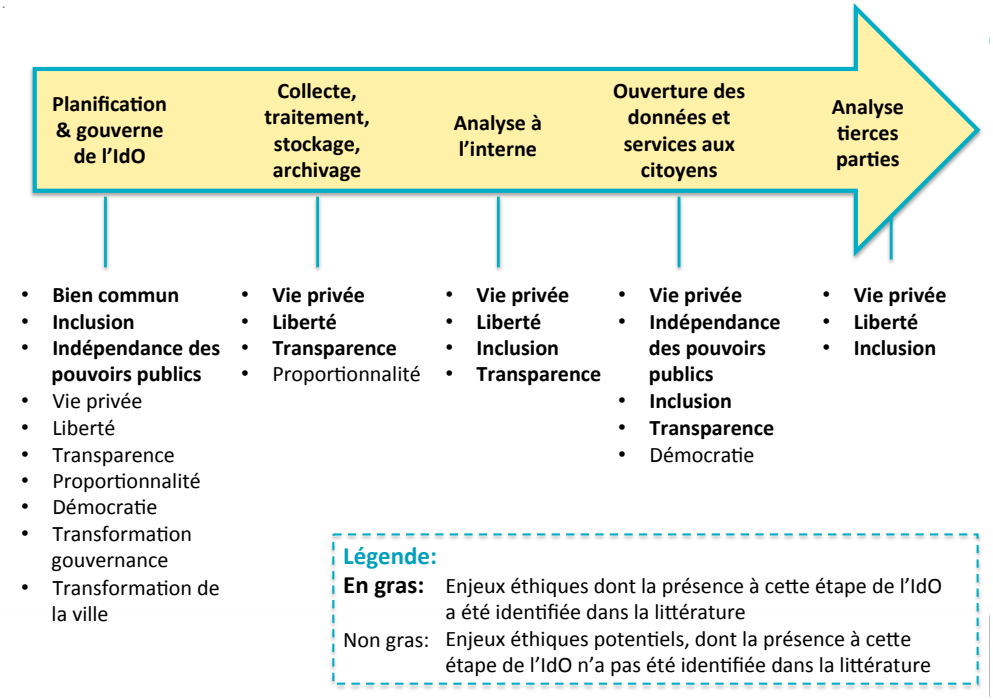


Figure 5: General Framework for Identifying Issues of Ethics and Social Acceptability

While a framework like the one presented below can serve in general considerations of this topic, it is useful to employ more specific frameworks that not only identify broad issues, but that list the activities and situations that could give rise to ethical or social issues. The following figures provide this detail. Figure 6 concerns issues and threats pertaining to privacy and transparency. Figure 7 deals with issues and threats pertaining to the common good, social inclusion, and separation of the government and business spheres. Figure 8 focuses on issues and threats pertaining to transformation of governance and the city.

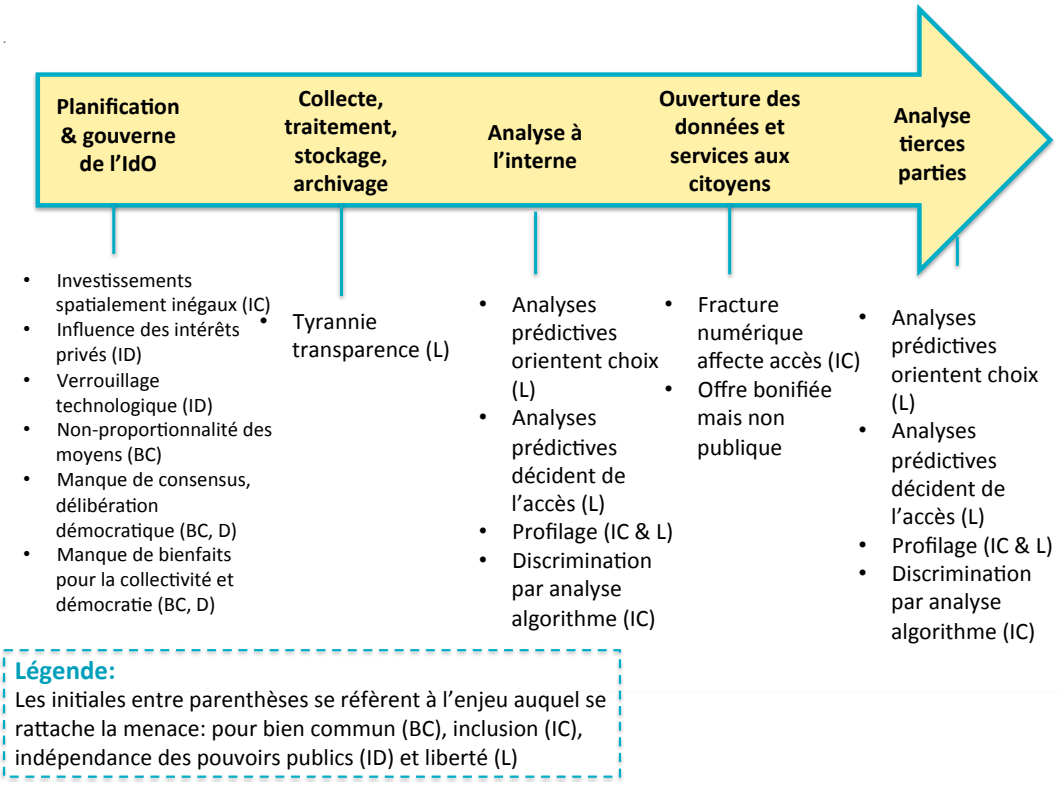


Figure 6: Threats Pertaining to Issues of the Common Good, Social Inclusion, Separation of the Government and Business Spheres and Freedom

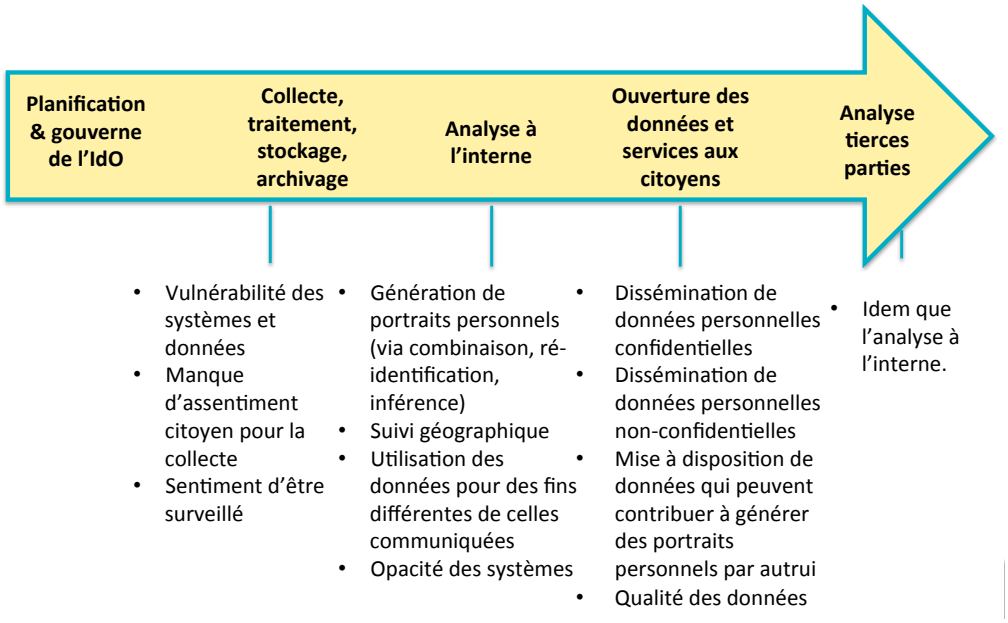


Figure 7. Threats Pertaining to Privacy and Transparency

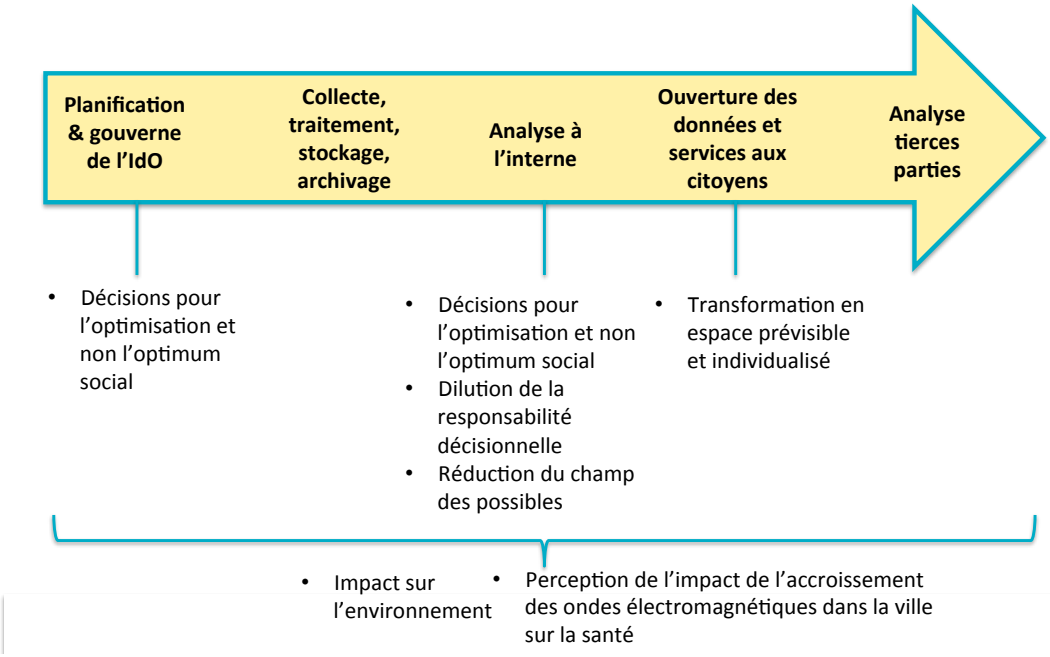


Figure 8: Threats Pertaining to Transformation of Governance and the City

3 Issue Analysis/Management Principles

The list of principles to apply in reviewing and managing issues is intended to incorporate the most relevant principles for dealing with issues of ethics and social acceptability due to the IoT project. The list provides guidance and basic rules for examining and dealing with the more difficult cases arising out of this project. These principles are intended to act as a roadmap in an environment characterized by change, innovation, transformation of the social bond and loss of ethical references.

3.1 Procedure

We decided to build on all existing guidelines pertaining to every technological and analytical component of the IoT system in developing this list, rather than start from scratch. We have accordingly considered the principles proposed for IoT, the smart city, artificial intelligence and big data research. We have studied these principles to identify overlaps among those identified in the literature, as well as others offering new and valuable perspectives. We ultimately developed a final list tailored to the system under consideration. We then compared our final list with the literature review to pinpoint further questions for study. The following box outlines our procedure, with each step considered in detail in the following sections.

Procedure for Developing the List of Principles

1. Create an inventory of existing relevant principles.
2. Extract and examine all principles, to understand their characteristics and see how they overlap.
3. Develop a final list of principles pertaining to IoT and the completeness with respect to other lists consulted.
4. Consider overlaps between the proposed list of principles and the literature review's findings.
5. Identify principles that should be enhanced and subsequent steps.

3.2 Inventory of Existing Principles, Along with Overlaps and Differences

Existing lists of principles were selected for:

- Their relevance to one or more technological or analytical components of the IoT system. In particular, we considered principles pertaining to big data, algorithms, artificial intelligence and information systems.
- Their ubiquitous mention in the literature, based on the frequency with which they were cited and references to them by other writers.

We primarily spoke to researchers and stakeholders in the field, but also performed Web searches[8] in making these selections. The four basic documents that contributed most to our study were: 1) Rob Kitchin's report (2016) "*Getting smarter about smart cities: Improving data privacy and data security.*" 2) Meg Leta Jones' article (2015) "*The Ironies of Automation Law: Tying Policy Knots with Fair Automation Principles*." 3) The report of the Commission de l'éthique en sciences et technologies du Québec sur les villes intelligentes (2017). 4) An interview with Kate Crawford in *Wired* magazine (Rosenburg, 2017) entitled *"Why AI is still waiting for its ethics transplant."*

The documents we ultimately selected came from a wide range of sources. Some contain general principles reflecting an international, Canadian or provincial consensus. Some are statements of principles from the municipal sector and academic forums. Others are codes of conduct.

The selected documents are listed in the following table and grouped according to the technological or topical components they concern. Section 3.3 then presents the lists of principles.

[8] We primarily used Google Scholar, since its does not automatically exclude grey literature, which this report presents as being of fundamental significance.

Table 1: Lists of Principles Considered

Category	Lists of Principles
General privacy principles	• Canadian PIPEDA fair information principles • Fair Information Practice Principles (FIPPs) • OECD Guidelines • Privacy by Design • Information and Privacy Commissioner of 7 Foundational Principles of Privacy by Design • City of Seattle Privacy Principles • EU general legislation of 1990 and 2018
General IoT and smart city principles	• Recommendations on smart cities in the Opinion of Québec's Commission en éthique sciences et technologie • NYC IoT Guidelines
Artificial intelligence principles[9]	• Asilomar AI Principles • Fair Automation Practice Principles (FAPPs) • The Montreal Declaration for a Responsible Development of Artificial Intelligence
Big data principles[10]	• Ten simple rules for responsible big data research
Codes of conduct	• ACM Code of Ethics and Professional Conduct • IEEE Code of Conduct[11]

We examined these lists to find overlaps between principles, as well as to distinguish the features of each. We began by entering all of the principles on an Excel spreadsheet. This resulted in 80 separate principles that we could group around common concepts. Appendix A presents the complete set of principles. We then identified overlaps between and differences among the principles, to extract a list of core principles backed by a certain consensus, while providing comprehensive coverage of the ethical issues identified in the literature. Section 4 presents this final list.

[9] The IEEE's deliberations (IEEE, 2017) on artificial intelligence can be added to this list for subsequent contributions to the inventory.

[10] The principles presented in the article by Richards and King (2014) could be added here for subsequent contributions to the inventory.

[11] ACM and IEEE jointly produced a code, but we did not cover it in this study. Since IEEE is in the process of creating a new version of its own code, we decided to stick to the latest codes, rather than those produced as part of a collaborative process.

3.3 Lists of Principles Considered

This section describes each of the lists considered, as appear in Table 1, above.

3.3.1 Canadian PIPEDA Fair Information Principles

The *Personal Information Protection and Electronic Documents Act* (Justice Canada, 2017) sets out Fair information principles.

This list was selected because it applies to all entities based in Canada and because these principles form the very core of Canadian privacy protection legislation.

Table 2: PIPEDA Fair Information Principles (Department of Justice Canada, 2017)

Principles	Explanation
Principle 1 - Accountability	An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.
Principle 2 - Identifying Purposes	The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.
Principle 3 - Consent	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
Principle 4 - Limiting Collection	The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
Principle 5 - Limiting Use, Disclosure, and Retention	Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes
Principle 6 - Accuracy	Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used
Principle 7 - Safeguards	Personal information must be protected by appropriate security relative to the sensitivity of the information.
Principle 8 - Openness	An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.
Principle 9 - Individual Access	Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Principle 10 - Challenging Compliance	An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

3.3.2 Fair Information Practice Principles (FIPPs) and OECD Guidelines

The *Fair Information Practice Principles* (FIPPs) and *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* are central to Canadian PIPEDA fair information principles (above), as well as principles governing most Western legislation in this area (Richards and King, 2014; Cate, 2006), making them fundamental principles.

FIPPs were published in the United States in 1973.[12] These five principles are also summarized as *openness, use limitation, individual participation (*right to obtain/correct data*), data quality and security safeguards*. FIPPs were eventually updated and enhanced in the form of the OECD Guidelines.

In his report presenting smart city privacy governance recommendations for Dublin, Rob Kitchin (2016) proposed basing its governance framework on FIPPs, OECD Guidelines and Privacy by Design principles (Kitchin, 2016). Kitchin did however note that several critics of the FIPPs and OECD Guidelines have claimed that these rules do not adequately address the issue of harm caused by predictive analysis, which is the result of inference, data sharing, reuse of data for new purposes and, generally, unpredictable data use in an age of big data. Furthermore, while *notice* and *consent* are included in FIPPs and the OECD Guidelines, it is generally acknowledged that they have not, to date, been truly effective in the smart city (Kitchin, 2016). We shall examine these points further in Section 4.

Since the Canadian standards appearing in Section 3.3.1 are largely drawn on the FIPPs and OECD Guidelines, these documents are quite similar. However, the following differences should be noted:

- The OECD Guidelines state that the use of personal data should not be incompatible with the purposes for which it was collected.
- The OECD Guidelines state that there should be a general policy of openness as to the identity and usual residence of the data controller.
- The OECD Guidelines state: "Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use."
- The OECD Guidelines include additional details on the form of openness with respect to personal data should take through the individual participation principle, as shown in the following figure:

Figure 9: OECD Guidelines Individual Participation Principles, Taken from CÉSTQ (2017)

Principe de la participation individuelle

13. Toute personne physique devrait avoir le droit :

a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;

b) de se faire communiquer les données la concernant;

i) dans un délai raisonnable;

ii) moyennant, éventuellement, une redevance modérée;

iii) selon des modalités raisonnables; et

iv) sous une forme qui lui soit aisément intelligible;

c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet; et

d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

[12] In the 1973 report "*Records, Computers, and the Rights of Citizens*," by the US government's *Advisory Committee on Automated Personal Data Systems*.

3.3.3 Privacy by Design and the Information and Privacy Commissioner of 7 Foundational Principles of Privacy by Design

In 2015, the Information and Privacy Commissioner of Ontario published a guide on privacy and personal information for municipal governments. The Commissioner proposed seven principles for municipalities to apply in these areas. The principles are quite similar to Privacy by Design rules, which enforce privacy protections by default. This means assuming that all data collected is, by default, private, unless citizens propose that it is not. This approach incorporates privacy principles in design specifications, IT uses, business practices, physical environments and system/application infrastructures (Cavoukian, 2012; Kitchin, 2016).

We selected the Ontario strategy since it is a Canadian initiative corresponding with the issues raised by urban IoT. It is also based on Privacy by Design, a key set of principles among the various efforts aimed at ensuring the protection of privacy in a smart city, as mentioned by Kitchin (2016) and many others. The European Union, the US Federal Trade Commission and several other national privacy protection commissioners (Kitchin, 2016) have adopted this approach.

Table 3: The Information and Privacy Commissioner of 7 Foundational Principles of Privacy by Design (Information and Privacy Commissioner of Ontario (2015)

Principle	Explanation
Proactive not Reactive	The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen.
Privacy as the Default Setting	We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact.
Privacy Embedded into Design	*Privacy by Design* is embedded into the design and architecture of IT systems and business practices.
Full Functionality — Positive-Sum, not Zero-Sum	*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.
End-to-End Security — Full Lifecycle Protection	*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved.
Visibility and Transparency — Keep it Open	*Privacy by Design* seeks to ensure that its component parts and operations remain visible and transparent, to users and providers alike
Respect for User Privacy — Keep it User-Centric	Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

3.3.4 City of Seattle Privacy Principles

Following months of consultations with stakeholders, Seattle adopted six privacy principles in February 2015. We selected this initiative because it constitutes one of the few attempts by a municipal government to establish basic principles applicable to smart city governance.

Of these principles, a few closely correspond with those presented in documents mentioned above, particularly with respect to the following concepts:

- Perform privacy impact assessments on new data programs.
- Allow people to have their data deleted.
- Ensure that subcontractors with access to personal data are subject to the city's privacy policies.

Seattle Privacy Principles

1. We value your privacy: Privacy impact assessments will be conducted on all new data programs.[13]
2. We collect and keep only what we need: The city only collects the information it needs to deliver city services.
3. How we use your information: When possible, the city makes available information about the ways it uses personal information and commits to giving people a choice whenever possible about how it uses their information.
4. We are accountable: The city complies with all federal and state privacy laws.
5. How we share your information: The city follows federal and state laws about information disclosure. Business partners and contracted vendors that receive or collect personal information from the city must agree to its privacy requirements.
6. Accuracy is important: The city works to correct inaccurate personal information, when practical.

The city consequently adopted a privacy commitment based on these six principles, applying privacy and data management practices to all its departments.

(Gaughan, 2016, p. 33)

3.3.5 Drawing on European Regulations

In 1990, the European Commission published the *Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.* This document serves as a roadmap for the adoption by member states of national legislation on the matter. This Directive, and the subsequent *General Data Protection Regulation* adopted in April 2016 (to be implemented in May 2018) are certainly complex pieces of legislation, resulting from deliberation and compromise. We have no intention of comprehensively analyzing or examining these texts, but will simply identify their main principles and in particular, those pertaining to issues that have so far received little or no consideration.

We selected the Directive and Regulation for this project because they focus on certain issues receiving little or no coverage in other frameworks or lists of principles. The Directive, for example, pertains to "knowledge of the logic involved in any . . . automated decisions" and proposes an independent supervisory authority—in the form of an outside agency that audits data management and use–and personal recourse in the event of damage. These principles are summarized in the following table:

[13] This commitment also requires an assessment of impact on privacy of the privacy threshold for all new data collection programs (Gaughan, 2016).

Table 4: Principles of the 1990 European Directive

Principes de la Directive européenne de 1990		
1	Limite des objectifs	Les données devraient être utilisées pour des fins spécifiques et subséquemment analysées ou communiquées seulement si ceci n'est pas incompatible avec les fins du transfert initial. Lorsque les données sont transférées pour des fins de marketing, les sujets des données devraient être en mesure de soustraire ses données si souhaité
2	Qualité des données et proportionalité	Les données devraient être précises et lorsque nécessaire maintenues à jour. Les données devraient être adéquates, pertinentes et non excessives en relation avec les objectifs pour lesquelles elles ont été transférées ou traitées
3	Transparence	Les individus devraient recevoir de l'information concernant les objectifs visés par le traitement des données et l'identité du contrôleur des données (…) et toute autre information nécessaire pour assurer la l'équité.
4	Sécurité	Les mesures de sécurité techniques et organisationnelles devraient être prises par le contrôleur de données, en fonction des risques présentées dans le traitement des données (…)
5	Accès, rectification et opposition	le sujet des données devrait avoir le droit d'obtenir une copie des données en lien avec lui/elle qui sont traitées et le droit de rectification lorsque les données ne sont pas précises. Dans certaines situations il devrait être en mesure de s'opposer au traitement de données en lien avec lui/elle.
6	Restriction sur les transferts ultérieurs	Il devrait être permis au récepteur des données initialement transférées de faire des transferts de données ultérieurs seulement dans les cas où le second récepteur (celui recevant le transfert ultérieur) est également sujet à des règles permettant un niveau adéquat de protection
7	Données sensibles	Lorsque des catégories sensibles de data sont impliquées (concernant les origines raciaux, ethniques, les opinions politiques, croyances religieuses, convictions philisophiques et éthiques (…) ou la santé et la vie sexuelle) des mesures de sécurité additionnelles devraient être en place, tel que le requis que les sujets des données donnent leur accord explicite pour le traitement des données.
8	Décision individuelle automatisée	Lorsque l'objectif du transfert est pour prendre une décision automatisée, l'individu devrait avoir le droit de connaître la logique impliquée dans la décision et d'autres mesurer devraient être prises pour sauvegarder l'intérêt légitime de l'individu.
Principes de mise en application accolés à la Directive		
1	Supervision indépendante	Les entités qui traitent des données personnelles ne sont pas seulement responsables mais aussi sujettes à une supervision indépendante, ayant l'autorité pour auditer les systèmes de traitement des données, investiguer les plaintes provenant d'individus et mettre en place des sanctions pour la non-conformité
2	Recours individuel	Les individus doivent avoir le droit de poursuivre légalement les contrôleurs de données et entités impliquées dans le traitement des données qui ne respectent pas la loi. Ils doivent avoir decours à la cour et aux investigations des agences gouvernemantales (...)

The Regulation, on the other hand, contains the following new concepts pertaining to the IoT system:

- Clear, affirmative consent.
- Right to erase data (if possible).
- Right to data portability.
- Privacy by Design.
- Notification of data breaches.
- Appointment of a data protection officer by public and private organizations.
- Mandatory data protection impact assessment for all activities that could have significant privacy implications.
- Encouragement in drawing up codes of conduct (European Parliament, 2016; Wikipedia, 2017).

3.3.6 Opinion of the Commission d'Éthique Sciences et Technologie du Québec sur la Ville Intelligente

In June 2017, the Commission d'éthique en sciences et technologie du Québec adopted an opinion entitled "La ville intelligente au service du bien commun : Lignes directrices pour allier l'éthique au numérique dans les municipalités du Québec" (CÉSTQ, 2017). The opinion proposes guidelines to promote development of smart cities working toward the common good and harmoniously combining ethical rules with the deployment of new technologies. This document was selected to contribute to that discussion, in view of its critical importance to deliberations on Québec-based smart cities and their technologies.

The Commission generally recommends building smart city policies around the following ethical principles:

- Maximize benefits for the common good.
- Eliminate or minimize possible potential damage to dignity, privacy and democracy.
- Ensure equitable distribution of potential benefits and drawbacks among those concerned.
- Ensure that expected benefits are also greater than drawbacks, including cost (CÉSTQ, 2017).

The Commission concluded its opinion by setting out values and principles to apply, as appear below. However, many of these values and principles relate more to the smart city than to IoT, itself. Furthermore, several of the items listed are similar to previously identified principles. Others, though, are new and quite pertinent, such as those concerning:

- Democracy (especially encouraging public participation in decisions and uses).
- The common good (especially public sector autonomy, precedence of the public interest, social inclusion, non-socialization of private service fees).
- Equity (especially equal treatment, special (territorial) justice, digital social inclusion.

Appendix B presents CÉSTQ's recommended values and principles.

3.3.7 NYC's Guidelines for Building a Smart + Equitable City

In 2016, New York City originally published the "*NYC's Guidelines for Building a Smart + Equitable City,"* pertaining to smart and equitable cities. They were subsequently adopted by more than 30 cities around the world, including Paris. These guidelines were designed to help municipal governments understand potential risks of IoT, promote uniform IoT deployment, provide transparency to the private sector and inform the public about the city's IoT strategy. These guidelines have been selected for their international recognition and their relevance to the central topic of this report. They are based on best practices and the experiences of over 50 cities around the world (NYC, undated).

The Guidelines consist of a blend of principles, operating procedures and management practices. They deal with ethical issues, as well as sound infrastructure governance. While their name highlights the smart city's role, the Guidelines actually focus on IoT deployment. The Guidelines are based on five principles described in detail in Appendix C.

Summary of NYC's Guidelines for Building a Smart + Equitable City

1. **Privacy + Transparency:** When we use new technologies on city streets and in public spaces, we are committed to being open and transparent about the "who, what, where, when, and why" for any data or information being collected and used.
2. **Data Management:** Data is the core of any IoT system. We will ensure that IoT and real-time data is captured, stored, verified, and made accessible in ways that maximize public benefit.
3. **Infrastructure:** To capitalize on the value and benefits derived from public assets, we will deploy, use, maintain and dispose of IoT devices, networks and infrastructure in an efficient, responsible, and secure manner.
4. **Security:** Keeping New Yorkers safe is our top priority. To do so, we are designing and operating IoT systems to protect the public, ensure the integrity of services, and maximize resilience.
5. **Operations + Sustainability:** We are committed to streamlining operational processes and ensuring financial, operational, and environmental sustainability to ensure that our city keeps running better and faster.

(NYC, 2017)

3.3.8 Asilomar Beneficial IA Principles

Asilomar's 23 principles were published in 2017, following the *Beneficial Artificial Intelligence Conference,* organized by the *Future of Life Institute*. This event brought together members of the academic and industrial sectors interested in artificial intelligence (Ai). The focus was technical, as well as economic, legal, ethical and philosophical.[14] They are listed as among the recently developed frameworks of principles to be considered for AI (Crawford, in Rosenburg, 2017).

The principles are intended to identify "what society should do to best manage AI in coming decades" (Future of Life Institute, 2017). Based on the literature and especially the latest reports on the subject from the academic, political and non-profit communities,[15] an initial draft list was developed prior to the event by conference organizers. This list was opened to comment and enhancement by conference attendees before and during the event, through discussion workshops on the topic, as well as a general survey. Only those principles endorsed by at least 90% of the participants were included in the final version, which is intended to stimulate discussion on perfecting the list and making it scalable.

These principles pertain to such topics of interest as:

- Ensuring that the security of systems is verifiable.
- System transparency and failure.
- Non-interference with social and civic processes.

These principles appear below (with some omitted to facilitate reading). The complete, original principles appear in Appendix D).

[14] It should be noted that various stakeholders associated with this initiative are highly critical of AI and believe it has the inherent potential to destroy humanity (as can be sensed in some of the principles they advocate). That view contrasts with the stances of those supporting, for example, the *Montréal Declaration*, which also covers AI, but sees it as a technological development to which guidelines should be applied (personal communication, 2017).

[15] For example, the *Stanford 100 Year Report*, recent White House reports and the *Partnership on AI* principles (Asilomar, 2017).

Table 5: Asilomar Beneficial IA Principles

Topic	Principles
From Research	
Research Goal:	The goal of AI research should be to create not undirected intelligence, but beneficial intelligence. Investments in AI should be accompanied by funding for research on ensuring its beneficial use.
Science-Policy Link:	There should be constructive and healthy exchange between AI researchers and policy-makers.
Research Culture:	A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.
Race Avoidance:	Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.
Ethics and Values	
Safety:	AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.
Failure Transparency:	If an AI system causes harm, it should be possible to ascertain why.
Judicial Transparency:	Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.
Responsibility:	Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.
Value Alignment:	Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.
Human Values:	AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.
Personal Privacy:	People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.
Liberty and Privacy:	The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.
Shared Benefit:	AI technologies should benefit and empower as many people as possible.
Shared Prosperity:	The economic prosperity created by AI should be shared broadly, to benefit all of humanity.
Human Control:	Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.
Non-subversion:	The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.
AI Arms Race:	An arms race in lethal autonomous weapons should be avoided.
Longer-Term Issues	
Capability Caution:	There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.
Importance:	Advanced AI could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources.
Risks:	Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.
Recursive Self-Improvement:	AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.
Common Good:	Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization.

(Future of Life Institute, 2017)

3.3.9 Fair Automation Practice Principles

Assistant Professor Meg Leta Jones (2015) proposed *Fair Automation Practice Principles* (FAPPs) to govern the development of autonomous objects, including automated decision-making systems and self-driving vehicles. These principles were inspired by FIPPs and several other core statements of principles, such as Richards and King's (2014) *Big Data Ethics* (privacy principles) and Riek and Howard's (2014) *A Code of Ethics for the Human-Robot Interaction Profession*. This list was selected because of its foothold in the literature, while being based on other existing frameworks that have been identified as relevant in this report or the preceding literature review.

These seven principles complement existing design practices, which take into account the actual use of objects and help identify areas where additional expertise may be needed (Jones, 2015, p. 121). Jones noted that automation principles cannot be defined in a vacuum. They must be collectively discussed and developed by designers, managers, users, investors, politicians, ethicists and legal scholars. The proposed principles serve, accordingly, as an invitation to a multiparty dialogue, rather than as a final list. Table 6, below, summarizes these principles.

In particular, these principles bring the following concepts to the discussion:

- Assessment of human risk, in recognition of the limits of existing resources.
- System transparency.
- Assurance that system failure is not surprising, silent or irresolvable.
- Testing for discriminatory impact.
- Consideration of impact to broader social values.
- Identification of predictable/unpredictable behaviour.

Table 6: Fair Automation Practice Principles (Jones, 2015)

Principles
Principle 1—Risk: Automated systems should not be deployed without an assessment of risks to the human in the loop or humans impacted by the loop. Identifying harms and understanding benefits is incredibly challenging but must not be left solely to technology companies, innovators, or developers. We should also be mindful of the fact that existing tools for risk assessment, cost-benefit analysis, and predictive are limited. They are focused on the short-term, knowable risks.
Principle 2—Transparency: Automated systems should be comprehensible and support situational awareness through effective transparency. Black boxes are bad design. When an operator does not know what a system is doing because of the opaqueness of its design, then error recognition, intervention, and resolution are timely and costly, if not impossible. Citron and Pasquale have argued for access to datasets, source code, programmer notes describing the variables, and correlations -- anything required to be able to meaningfully assess systems whose predictions change pursuant to AI logic (Jones, 2015, p. 125).
Principle 3—Errors and Limitations: Automated system failures should not be surprising, silent, or irresolvable. Situational awareness, mental workload, skill degradation, and automation bias must be considered when designing error detection and considering limitations. Citron's work on public benefit systems reveals a large number of errors occurring without any good way to alert operators or resolve issues in a timely manner.
Principle 4—Diversity and Discrimination: Automated systems should reflect on biases and choices during design and test for discriminatory impacts and diverse users.
Principle 5—Sensitive Situations: Automated systems should account for sensitive situations and information preferences of the humans in the loop. Sensitive situations, like those that deal with sensitive information, private places, or vulnerable populations should be assessed with an appropriate level of care and expertise.
Principle 6—Man-Machine Comparison An automated system's design and implementation should locate the human in the loop and reassess the system's impact on the human and larger social values. We must consider humans to be imperfect. A discussion of what critical decisions are to be made by humans (and why) and how to limit automation bias and moral buffers in those instances would be an incredible contribution to the guidance of automation.
Principle 7—Predictability: Automated systems should be initially and continually inventoried for predictable and unpredictable behavior.

3.3.10 The Montreal Declaration for a Responsible Development of Artificial Intelligence

The Montreal Declaration for a Responsible Development of Artificial Intelligence was published in November 2017, at the conclusion of the Forum on the Socially Responsible Development of Artificial Intelligence. Drafted by a group of the Forum's organizers, including researchers from various fields related to AI, the Declaration is designed to promote dialogue among the public, experts and government representatives on artificial intelligence in Québec (Forum on Socially Responsible AI, 2017).

The Declaration identifies seven values—well-being, autonomy, justice, privacy, knowledge, democracy and responsibility—accompanied by a set of questions for each, intended to explore that value's relationship to AI's development. For each value, a general principle is also proposed, although it does not always directly address the questions raised. The Declaration appears in full in Appendix E.

The Declaration was selected because of its geographic origin and Montréal's importance in the international chessboard of AI development.

Table 7: Extract from the Montréal Declaration

Value and Proposed Principle	Questions
Well-being: Proposed principle: The development of AI should ultimately promote the well-being of all sentient creatures.	**Questions:** • How can AI contribute to personal well-being? • Is it acceptable for an autonomous weapon to kill a human being? What about an animal? • Is it acceptable for AI to control the running of an abattoir? • (etc.)
Autonomy: Proposed principle: The development of AI should promote the autonomy of all human beings and control, in a responsible way, the autonomy of computer systems.	• How can AI contribute to greater autonomy for human beings? • Must we fight against the phenomenon of attention-seeking which has accompanied advances in AI? • Should we be worried that humans prefer the company of AI to that of other humans or animals? • (etc.)
Justice: Proposed principle: The development of AI should promote justice and seek to eliminate all types of discrimination, notably those linked to gender, age, mental / physical abilities, sexual orientation, ethnic / social origins and religious beliefs.	• How do we ensure that the benefits of AI are available to everyone? • Must we fight against the concentration of power and wealth in the hands of a small number of AI companies? • What types of discrimination could AI create or exacerbate? • Should the development of AI be neutral or should it seek to reduce social and economic inequalities? • What types of legal decisions can we delegate to AI?
Privacy: Privacy: Proposed principle: The development of AI should offer guarantees respecting personal privacy and allowing people who use it to access their personal data as well	• How can AI guarantee respect for personal privacy? • Do our personal data belong to us and should we have the right to delete them? • Should we know with whom our personal data are shared and, more generally, who is using these data?

as the kinds of information that any algorithm might use	• Does it contravene ethical guidelines or social etiquette for AI to answer our e-mails for us? • What else could AI do in our name?
Knowledge: Proposed principle: The development of AI should promote critical thinking and protect us from propaganda and manipulation.	• Does the development of AI put critical thinking at risk? • How do we minimize the dissemination of fake news or misleading information? • Should research results on AI, whether positive or negative, be made available and accessible • (etc.)
Democracy: Proposed principle: The development of AI should promote informed participation in public life, cooperation and democratic debate.	• How should AI research and its applications, at the institutional level, be controlled? • In what areas would this be most pertinent? • Who should decide, and according to which modalities, the norms and moral values determining this control? • (etc.)
Responsibility: Proposed Principle: The various players in the development of AI should assume their responsibility by working against the risks arising from their technological innovations. (The Forum on the Socially Responsible Development of Artificial Intelligence, 2017)	• Who is responsible for the consequences of the development of AI? • How should we define progressive or conservative development of AI? • How should we react when faced with AI's predictable consequences on the labour market? • (etc.)

3.3.11 Ten Simple Rules for Responsible Big Data Research

The Council for Big Data, Ethics, and Society, a group of 20 internationally renowned researchers in the social, natural and computer sciences proposed these 10 rules. They are partly drawn on the *Ten Simple Rules* of PLOS Computational Biology. The first five were developed to reduce the possibility of harm due to big data research practices. The *Council for Big Data, Ethics, and Society's* exemplary reputation in the field of critical analysis of big data and the number of leading researchers who have endorsed the Ten Rules makes this a fundamental document.

In terms of advanced concepts, the Ten Simple Rules bring several new ideas to the table, such as:

- The notion that privacy is not binary. Privacy is contextual, situational and not reducible to a public vs. private scenario. Privacy can pertain to groups, as well as individuals.
- Preventing data re-identification is crucial.
- Difficult ethical choices must be debated and perceived as being an integral part of the effort.
- Organizing/developing data and systems to audit it.
- Engaging, to understand and participate in the broader implications of data and analytical practices.

Ten Simple Rules for Responsible Big Data Research (Summary)

1. Acknowledge that data are people and can do harm.
2. Recognize that privacy is more than a binary value: privacy is contextual and situational, not reducible to a simple public/private binary. Privacy also goes beyond single individuals and extends to groups. This is particularly resonant for communities who have been on the receiving end of discriminatory data-driven policies historically, such as the practice of redlining.
3. Guard against the re-identification of your data . . . Identify possible vectors of re-identification in your data . . .
4. Practice ethical data sharing.
5. Consider the strengths and limitations of your data; big does not automatically mean better.
6. Rather than a bug, the lack of clear-cut solutions and governance protocols should be more appropriately understood as a feature that researchers should embrace within their own work.
7. Develop a code of conduct for your organization, research community, or industry . . . as a way of cementing this in daily practice.
8. Design your data and systems for auditability.
9. Engage with the broader consequences of data and analysis practices.
10. Know when to break these rules

(Zook, et al., 2017)

3.3.12 ACM Code of Ethics and Professional Conduct

In 1992, the ACM (*Association for Computing Machinery*) published its first *Code of Ethics and Professional Conduct*, which it is now updating (scheduled for 2018). The Code was designed to support IT professionals and is divided into four sections. Section 1 deals with basic ethical issues. Section 2 concerns professional responsibility. Section 3 deals with the roles of individuals with leadership positions in the workplace or in a professional capacity. Section 4 concludes with principles for ensuring compliance with the Code.

The Code's 2018 version is summarized in the following table and presented in full in Appendix F. It contributes several useful ideas for consideration. For one thing, the detail given to each principle and the way principles are broken down into daily practices in the information sector, provides potentially useful clarifications. The Code also highlights the following factors:

- Ensuring that IT hardware and strategies are applied by third parties in a socially responsible manner.
- Emphasizing honesty and confidence, particularly in terms of data manipulation/creation.
- Taking action not to discriminate through data analysis.

The ACM Code was selected because it has been repeatedly cited as a reference for concrete initiatives to address ethical issues in the engineering and the computer sciences.

General Moral Principles

A computing professional should…

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. Computing professionals should give consideration to whether the products of their efforts will be used in socially responsible ways, will meet social needs, and will be broadly accessible.

1.2 Avoid harm.

In this document, "harm" means negative consequences to any stakeholder, especially when those consequences are significant and unjust. Examples of harm include unjustified death, unjustified loss of information, and unjustified damage to property, reputation, or the environment. This list is not exhaustive.

1.3 Be honest and trustworthy.

Honesty is an essential component of trust. A computing professional should be fair and not make deliberately false or misleading claims and should provide full disclosure of all pertinent system limitations and potential problems. Fabrication of data, falsification of data, and scientific misconduct are similarly violations of the Code.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and equal justice govern this principle. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of ACM policy.

1.5 Respect the work required to produce new ideas, inventions, and other creative and computing artifacts.

1.6 Respect privacy.

"Privacy" is a multi-faceted concept and a computing professional should become conversant in its various definitions and forms.

This requires taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals or groups. Computing professionals should establish procedures that allow individuals to review their personal data, correct inaccuracies, and opt out of automatic data collection.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined and enforced, and personal information gathered for a specific purpose should not be used for other purposes without consent of the individual(s). When data collections are merged, computing professionals should take special care for privacy. Individuals may be readily identifiable when several data collections are merged, even though those individuals are not identifiable in any one of those collections in isolation.

1.7 Honor confidentiality.

Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code.

(ACM, current version for 2018)

3.3.13 IEEE Code of Conduct

The IEEE (Institute of Electrical and Electronics Engineers), first established in the US, is the world's leading professional technological association (IEEE, 2017b). It is the "voice" of engineering, computer science and information technologies around the world. However, its American origins are still prominent, in terms of its membership and political positions.

The IEEE Code of Conduct has 10 principles. They are important, because they were developed to be applied by IT specialists. They also cover other topics not relevant here and not covered by other lists of principles:

- The responsibility to disclose promptly factors that might endanger the public or the environment.
- To be honest and realistic in stating claims or estimates based on available data.

The IEEE Code was selected because it has repeatedly been cited as a reference in terms of concrete measures for addressing ethical issues in engineering and the computer sciences.

IEEE Code of Conduct (summary)

1. to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics;

(IEEE, 2017)

4 List of Proposed Principles

The final list of principles proposed in this report was developed in consideration of all principles discussed in Section 3.3. These principles were then classified, summarized and distilled to produce a final list, based on the following criteria:

- Comprehensiveness: cover a maximum of issues identified in the list of principles consulted.
- Relevance: all issues pertaining directly to the management of ethical issues and the IoT system's various technological components.[16]
- General to specific: Identify a limited number of general principles and break them down to more specific ones.

Obviously, this proposed framework is intended as a starting point. It must evolve and become more robust through consultation/verification of other reference documents, deliberations within Montréal and broader consultations with stakeholders.

The following table presents the general principles proposed. They can then be broken down into specific principles (subprinciples), as appears in Appendix G. Most of the proposed principles are based on Canadian PIPEDA fair information principles, CÉSTQ's opinion on smart cities (with respect to the common good, democracy and public participation, government autonomy) and the *NYC's Guidelines for Building a Smart + Equitable City*.

This list should comprise the key principles for guiding the study and management of ethical and social issues involved in the technological and analytical systems of urban IoT. These principles incorporate the topics that pertain to the system in question, selected from the 13 existing lists, other than the last principle concerning freedom. As described in Section 4.1, freedom was added since this issue, which was identified in the literature review (Russo Garrido, et al., 2017), is not comprehensively covered by the lists we consulted.

[16] However, principles pertaining to general good IoT governance (in terms of infrastructure maintenance, effectiveness, etc.), have been excluded.

Table 8: List of 11 Principles

Thème	Principe
Bien commun	Assurer que l'IdO soit au service du bien commun et de la recherche d'un optimum social.
Démocratie et participation citoyenne	Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique
Vie privée	Protéger et respecter la vie privée* des citoyens
Transparence	Être transparent sur le « qui, quoi, quand, où, pourquoi et comment » de la collecte, la transmission, le traitement et l'utilisation
Sécurité	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Bonne gestion des données	Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques
Évaluations et conséquences	Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données et veiller à l'analyse des conséquences à long terme sur les valeurs sociales élargies
Équité et inclusion	Mettre tous les moyens en œuvre pour que le traitement accordé tous soit juste et impartial. Éviter le profilage, la discrimination et le renforcement des inégalités pour développer un projet inclusif
Autonomie des pouvoirs publics	Assurer l'autonomie de la sphère publique et la primauté de l'intérêt public par rapport aux intérêts privés
Systèmes explicables	Concevoir des systèmes auditables et dans des cas de prise de décision automatisée, donner aux individus accès aux logiques qui président dans la décision, ainsi qu'une explication des données utilisées (quelle donnée, quelle source, comment est-elle mobilisée)
Liberté	Assurer que le citoyen puisse préserver son sentiment de liberté

*There has been much debate over defining privacy. In this report, the term refers to personal freedom against any physical intrusion, any interference in personal life and any impediment to a person's ability to control the access and use of their personal information.

Specific principles, derived from each of the major principles appearing above, are presented in Appendix G. This appendix also identifies the sources of these proposed major principles (the list, framework or code from which they were taken), along with the lists of principles consulted, which overlap in different areas.

We have adopted a comprehensive, well-documented approach to selecting specific principles. Our choices were accordingly designed to define a maximum number of specific principles pertaining to urban IoT, while eliminating possible duplications among overly similar rules. Determining the final principles and desired levels of specificity is up to the city.

A portion of Appendix G is reproduced in Figure 12, listing the general and specific principles identified. This extract appears again in Figure 13, this time highlighting the sources for each identified principle.

Figure 10: Extract of Excel Spreadsheet Highlights Major and Specific Principles (See complete spreadsheet in Appendix G)

Compilation - Principes retenus

Principe	Détails	Sous-détails	Sources								
Bien commun											
Assurer que l'IDO soit au service du bien commun et de la démocrati											
	Le projet de l'IdO doit entraîner des bénéfices po								CÉQ		
	Le projet de l'IdO doit se fonder sur la conciliatio								CÉQ		
	Le projet de l'IdO doit être proportionnel aux ob								CÉQ (voir formulation)		
	Les coûts ne doivent pas être socialisés alors que								CÉQ		
Démocratie et participation citoyenne											
Promouvoir la participation citoyenne pour définir une vision concer									CÉQ		
	La participation et l'engagement des citoyens et								CÉQ		
	Le projet de l'IdO doit contribuer à améliorer les								CÉQ		
	Droit à soustraire ses données: Donner aux citoy					Euro 2018	Seattle				
	Débattre des décisions éthiques difficiles: plutôt										
Respecter la vie privée											ACM (
Protéger et respecter la vie privée des citoyens											
	Détermination des fins de la collecte: Informer le		Canada							Lignes IdO (s	
	Consentement: Les informations doivent être co		Canada	FIPPs		Euro 2018	Seattle				ACM
	Limitation de la collecte: L'organisation ne peut		Canada	FIPPs		Euro 1990	Seattle				ACM
	Utilisation pour les fins annoncées: Les renseign		Canada	FIPPs		Euro 1990				same	ACM
	Durée de vie des données: On ne doit conserver		Canada							Lignes IdO (formulation in	ACM
	Qualité de données: Les renseignements person		Canada	FIPPs		Euro 1990			CÉQ (à deux endroits)		ACM
	Vie privée par défaut: Respecter la vie privée cor				Ontario			Priv b Design			
		Anonymisation: les renseign								Lignes IdO	
		Éviter la réidentification des									
		Favoriser les informations o								Lignes IdO	

Figure 11: Extract of Excel Spreadsheet Highlighting Specific Principles and their Sources (See complete spreadsheet in Appendix G)

Compilation - Principes retenus

Principe	Détails	Sous-détails
Bien commun		
Assurer que l'IDO soit au service du bien commun et de la démocratie (inspiré de CÉSTQ)		
	Le projet de l'IdO doit entraîner des bénéfices pour la collectivité (CÉSTQ) (inspiré Asilomar, FAPPs)	
	Le projet de l'IdO doit se fonder sur la conciliation des valeurs, perspectives, intérêts pluriels présents dans la société civile et sur la recherche	
	Le projet de l'IdO doit être proportionnel aux objectifs visés (CÉSTQ)	
	Les coûts ne doivent pas être socialisés alors que les bénéfices sont privatisés (équité)(CÉSTQ)	
Démocratie et participation citoyenne		
Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique (inspi		
	La participation et l'engagement des citoyens et des groupes qui les représentent sont nécessaires pour définir une vision concertée (CÉSTQ)	
	Le projet de l'IdO doit contribuer à améliorer les pratiques démocratiques, mais aussi être objet de la délibération démocratique (CÉSTQ, FAP	
	Droit à soustraire ses données: Donner aux citoyens la possibilité de soustraire leurs données lorsque possible (Seattle, Euro 2018)	
	Débattre des décisions éthiques difficiles: plutôt que de les voir comme des problèmes, l'absence de solutions évidentes et protocoles de gou	
Respecter la vie privée		
Protéger et respecter la vie privée des citoyens		
	Détermination des fins de la collecte: Informer le sujet des informations collectées et de la finalité de la collecte avant ou lors de la collecte (N	
	Consentement: Les informations doivent être collectées avec le consentement des individus (Normes Canada - FIPPs, OCDE, ACM)	
	Limitation de la collecte: L'organisation ne peut recueillir que les informations nécessaires aux fins déterminées et doit procéder de façon hon	
	Utilisation pour les fins annoncées: Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles a	
	Durée de vie des données: On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fin:	
	Qualité de données: Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont dest	
	Vie privée par défaut: Respecter la vie privée comme paramètre par défaut - automatique protégé (Ontario, VPDC)	
		Anonymisation: les renseignements personnels devraient être anonymisés par défaut avant de rendre l'information publ
		Éviter la réidentification des données: notamment en identifiant les possibles vecteurs de réidentification des données
		Favoriser les informations ouvertes anonymisées et agrégées (Lignes IdO)
		Vie privée dans un environnement de données massives: Lorsque des bases de données sont croisées, considérer les per
		Les tierces parties sous-contractées ayant accès aux données personnelles devront se soumettre à la politique de la vie p
	Vie privée dès la conception (Ontario, VPDC)	

4.1 Analysis of Overlaps Between the Proposed Framework and the Literature Review

We studied overlaps between our framework and review of the literature to enhance our final list of principles (Russo Garrido, et al., 2017). Consequently, issues and threats identified in the literature review and not (or only partially) covered in the lists/frameworks consulted have been listed.

As previously mentioned, the key ethical and social issues identified in the literature review are privacy, reliability/transparency, social inclusion, separation of the government and business spheres, freedom, change in governance and transformation of the city.

Generally, the proposed set of principles provides good coverage of documented issues, as well as related threats identified in the literature review (as appear in Figures 2, 3 and 4). Overlaps and gaps can be summarized as:

- Transparency, social inclusion and separation of the government and business spheres, as described in the literature review, are covered by the proposed framework.
- Privacy and change in governance, as described in the literature review, are covered by the proposed framework (under the headings of privacy, security, common good), but certain principles should be included (minor additions) to achieve complete coverage.
- Freedom is not covered by the proposed framework, outside the protection of privacy. Some additions should be made to the general and complete principles to achieve complete coverage.
- The framework only partly covers transformation of the city (through the “common good” principle). Some specific principles should be added to achieve complete coverage.

The following table lists draft principles to be added to the final list. These additions appear in Appendix G and in Table 8,[17] above.

Table 9: Additional Principles Identified in the Literature Review

Enjeux de la liberté dans la revue de littérature
Assurer que le citoyen ne fasse pas constamment l'objet de suivi dans sa vie quotidienne et l'informer du suivi effectué
Assurer que le citoyen ait pleinement le choix de ne pas dépendre d'analyses prédictives qui orientent ses choix
Assurer que les situations dans lesquelles l'accès des citoyens soit décidé par le biais d'analyses perscriptives soient limités, documentés de façon accessible au citoyen et puissent faire l'objet de recours de la part du citoyen, dans des délais raisonnables
Enjeux de la transformation de la ville dans la revue de littérature - classés sous bien commun dans la liste de principes
Comprendre les perceptions et craintes de la population montréalaise par rapport au projet de l'IdO
Veiller à l’analyse des conséquences à long terme du projet de l'IdO sur les valeurs sociales élargies (FAPPs) et sur l'environnement, en particulier l'émission des GES occasionnées par le projet, à travers le monde
Toute décision émanant du projet de l'IdO doit être rattachée à responsabilité décisionnelle humaine
Le projet de l'IdO doit viser l'optimum social - pas seulement l'optimisation des services/processus
Les preneurs de décisions municipaux doivent être conscients des angles morts existant dans les données et projets (ex: amélioration des services) liés à l'IdO, en particulier par rapport aux populations vulnérables
Le projet de l'IdO doit contribuer à la cohésion sociale, plutôt que l'individualisation de la ville

[17] Table 8 only considers major (not specific) principles. The only change needed was adding a principle pertaining to freedom.

4.2 Next Steps in Developing the Framework

Although our proposed list of principles is the result of a meticulous effort to bring together existing principles for addressing ethical and social issues of the IoT system, as planned for Montréal, further work is required to complete this list and make it fully useful. Sections 4.2.1 and 4.2.2 describe recommended future measures for continuously improving the list.

4.2.1 Enhancing Certain Principles

Although the proposed list of principles incorporates relevant principles found in existing lists, some of them are now viewed as being ineffective or warranting enhancement. These principles all pertain to privacy, including:

- Stating why the data is being collected.
- Consent before or during collection.
- Limiting data collection to pre-established purposes.
- Considering potential threats to privacy by cross-referencing data.

As discussed in detail in the literature review (Russo Garrido, et al., 2017), the first three principles are consistent with data privacy management principles that have been in force for the past few decades. However, all of these principles directly conflict with many IoT system goals and are not highly viable in an urban environment in which data is constantly being captured.

Limiting data collection and pre-establishing the reasons for it constitute major stakes for a big data project in which data quantities are synonymous with the project's potential and where data reuse is intended, to stimulate innovation. IoT, in other words, challenges our understanding of data by being "infinitely connectable, indefinitely repurposable, continuously updatable and easily removed from the context of collection." (Metcalf and Crawford, 2016).[18]

It is also difficult to define consent in practical terms, in an environment where data is constantly being captured and it is difficult to obtain the personal consent of all persons affected by such collection. Finally, although potential threats to privacy from cross-referencing data are recognized as posing a huge challenge, it is not clear how this principle can be effectively applied, in practice. Furthermore, deliberation and research is needed to determine how to make these principles practical and relevant again in municipal governance.

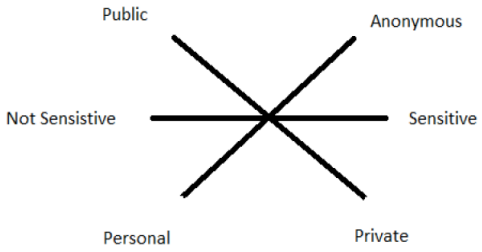
Resolving all of these questions would require, it seems, rethinking the very boundaries of what is commonly understood to be privacy in a public space like the city. Privacy is often associated with the concepts of intimacy, home life and personal information. However, the possibility of gather information about individuals in public areas raises the question of if such information is private or not and under what circumstances it might be.

[18] This quote originally applied to big data. However, it equally applies to the IoT system, which employs big data.

Helen Nissenbaum advanced the idea that privacy is primarily based on information exchanges, which give rise to standards specific to such exchanges (Nissenbaum, 2004; Barocas and Nissenbaum, 2014). Information may or may not be shared without violating privacy, depending on the interaction between various factors, such as relations between the parties concerned, the information's sensitivity and the direction of exchange (two- or one-way),[19] as illustrated in the following figure. Privacy is not "either-or." It depends more on the context that the type of information communicated. Consequently, Nissenbaum (2014) argued that individuals might be entitled to privacy in a public space.

[19] This is known as the *contextual integrity principle* (Barocas and Nissenbaum, 2014). For example, data rules for a healthcare unit, establishing the kinds of information that can be shared by stakeholders (patient, doctor, administrative staff, family). Under these circumstances, patients who provide access to their personal information can do so in confidence if this data is handled according to the rules and social expectations on disclosure, communication and confidentiality.

Figure 12: Certain Contextual Privacy Factors Considered (Gaughan, 2016, 17).



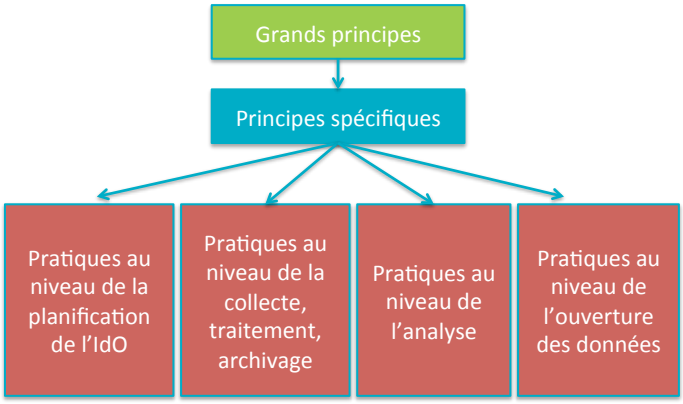
The researchers believe that putting privacy in the context of an exchange, rather than as an "either-or," could help solve the difficult problem of "what to do" with certain frequently cited privacy principles that are clearly outmoded and inadequate in current circumstances.

4.2.2 Next Steps Planned

The following steps are proposed for expanding the list are generally aimed at discussing, selecting, validating and enhancing the suggested principles. They include:

- Discussing and validating the 10 proposed principles.
- Discussing, reformulating, selecting and validating the identified specific principles. In particular, it will be necessary to determine the level of specificity desired and it is preferable to give some specific principles more weight than others. The final wording should be planned to produce optimal guidelines.
- Identifying any missing specific principles, through such means as detecting overlaps among the different reference documents and their applicability to the various phases of the IoT system. This effort would involve an in-depth study of possibly missing principles. As previously presented, our list of principles is based on existing lists, frameworks and codes. Consequently, its coverage and blind spots reflect existing lists. The list of principles should, accordingly, be given critical, detailed examination to identify any gaps.
- Enhancing weak specific principles—as discussed in Section 4.2.1
- Taking the discussion on the list of principles beyond city hall—as was the case of Seattle, which brought together members of civil society in developing its privacy principles. Montréal would benefit by including stakeholders to discuss and share their ideas on the proposed framework. These acts could play a role in debating and contributing to placing the IoT project in the hands of the community.
- Identifying how the framework breaks downs into specific practices at each phase of the IoT system, as shown in Figure 13. It is essential that the stated principles can be subdivided into specific practices applicable to the daily routines of city officials.

Figure 13: Major Principles Broken Down into Specific and Practical Principles



5 Conclusion

The frameworks proposed in this report are intended to contribute to Montréal's efforts to develop one or more conceptual frameworks for ethical governance of an IoT system. The first objective is designed to support decision-makers in identifying existing and emerging issues of ethics and social acceptability. The second is intended to delineate general and specific principles that could serve as good to guide Montréal in developing a set of municipal principles to apply in considering and managing ethical issues.

As previously mentioned, these principles are not, on their own, complete conceptual frameworks. However, they are important milestones in developing a more comprehensive, scalable framework. These principles could ultimately make an important contribution in implementing best practices for examining, managing and responding to issues of ethics and social acceptability pertaining to Montréal's IoT system. This is because we must acquire resources to assist in the ongoing monitoring of emerging issues and develop appropriate principles and practices to support deliberations on approaches to take and social choices to be made, in contending with the uncertainty and social change arising out of the deployment of new technologies in the city.

6 Bibliography

ACM (2017), The 2018 ACM Code of Ethics and Professional Conduct: Draft 2. Update of the ACM Council 10/16/92. Viewed at: https://ethics.acm.org/2018-code-draft-2/. Consulted December 20, 2017.

Future of Life Institute (2017), *Asilomar AI Principles*. Viewed at: https://futureoflife.org/ai-principles/ Consulted December 20, 2017.

Cate, Fred. H. (2006), "The Failure of Fair Information Practice Principles," In *Consumer Protection in the Age of the Information Economy*. pp. 343-379.

Cavoukian, Ann (2012), "*Privacy by Design*," *IEEE Technology and Society Magazine*, 31:4, pp. 18-19.

CÉSTQ (2017), *La Vielle intelligente au service du bien commun : Lignes directrices pour allier l'éthique au numérique dans les municipalités du Québec*, Gouvernement du Québec, 112 pp.

Information and Privacy Commissioner of Ontario (2015), *Transparency, Privacy and the Internet: Municipal Balancing Acts*, Ontario government, 24 pp.

European Parliament (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and the Free Movement of Such Data*, European Union.

The Forum on the Socially Responsible Development of Artificial Intelligence (2017), *The Montreal Declaration for a Responsible Development of Artificial Intelligence,* Viewed at: https://www.declarationmontreal-iaresponsable.com/la-declaration, Consulted December 20, 2017.

Gaughan, M (2016), *Privacy in the Smart City: Implications of Sensor Network Design, Law, and Policy For Locational Privacy*, Master's thesis, Urban Studies, University of Washington.

IEEE (2017), *Code of Ethics and Professional Conduct*, Viewed at:
https://www.ieee.org/about/corporate/governance/p7-8.html, consulted December 20, 2017.

IEEE (2017b), *IEEE Mission and Vision*, Viewed at: https://www.ieee.org/about/vision_mission.html Consulted December 20, 2017.

Jones, M.L. (2015), "The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles," *Vand. J. Ent. & Tech. L.*, Vol. 18, pp. 77-193.

Kitchin, R (2016), *Getting smarter about smart cities: Improving data privacy and data security*, Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Metcalf, J. and Crawford, K. (2016), "Where are human subjects in big data research? The emerging ethics divide," *Big Data & Society*, January-June, pp. 1-14.

Justice Canada (2017), "Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96," in *CANADA, Personal Information Protection and Electronic Documents Act*: S.C. 2000, c. 5, current as of July 3, 2017 [Ottawa], Justice Canada, 2017, Appendix 1, article 5.

New York City (2017), *NYC's Guidelines for Building a Smart + Equitable City*, Viewed at: https://iot.cityofnewyork.us Consulted December 20, 2017.

New York City Innovation & Technologies Workgroup (undated), *NYC's Guidelines for Building a Smart + Equitable City*, The NYS Forum.

OECD (2013), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Viewed at: http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm Consulted December 20, 2017.

Richards, N. M. and King, J. H. (2014), "Big Data Ethics," *Wake Forest Law Review* 49: 393-432.

Riek L. and Hartzog, W. and Howard D., et al. (2014), "The Emerging Policy and Ethics of Human Robot Interaction," *Proceedings of the Tenth Annual ACM/IEEE International Conference on Human-Robot Interaction Extended Abstracts*, March 2, 2015, pp. 247-248

Rosenberg, Scott (2017), "Why AI Is Still Waiting For Its Ethics Transplant," *Wired*, November 2017. Viewed at:https://www.wired.com/story/why-ai-is-still-waiting-for-its-ethics-transplant/?mbid=email_onsiteshare Consulted December 20, 2017.

Russo Garrido, S., Allard, M.C., Merveille, N., et al. (2017), *Final Report #1 for Batch 5 of the IoT Standards Development Project Literature Review: Ethical Issues And Social Acceptability of IoT in the Smart City*, Report delivered to Jean-Martin Thibault in November 2017.

Zook, M., Barocas, S., Boyd, D., Crawford, K., Keller, E., Gangadharan, S.P., et al., e1005399 (2017), "Ten simple rules for responsible big data research," Editorial, *PLOS Computational Biology* 13(3).

Appendix A
Complete List of Principles Considered for Analysis

This Appendix appears below under the second tab of the Excel file *Compilation finale principles 10 12 2017*

Appendix B
Values and Principles of Smart Cities Serving the Common Good (CÉSTQ, 2017)

B. Values and Principles of the Commission d 'Éthique Sciences et Technologie du Québec, in Its Opinion on Smart Cities (2017)

Démocratie

- ☐ L'autorité publique doit répondre à des exigences de légitimité démocratique et faire usage de sa souveraineté sur son territoire en conséquence. Les individus ne sont pas que des consommateurs de services publics, mais aussi, et surtout, des acteurs politiques.
- ☐ L'autorité publique est soumise à des normes éthiques de responsabilisation, de confiance, de transparence, de poursuite du bien commun et d'inclusion.
- ☐ L'utilisation d'un moyen numérique comme soutien aux dimensions participative, délibérative, représentative ou décisionnelle doit assurer l'inclusion du plus grand nombre de citoyens et de points de vue possible, et non une surreprésentation de la portion la plus « branchée » de la population.
- ☐ Le numérique doit être non seulement un moyen d'améliorer les pratiques démocratiques, mais aussi un objet de la délibération démocratique.
- ☐ « [L]a participation et l'engagement des citoyens et des groupes qui les représentent sont nécessaires pour définir une vision concertée du développement et assurer sa durabilité sur les plans environnemental, social et économique ».

  ↳ *– Loi sur le développement durable, art. 6 e) « participation et engagement »*

Subsidiarité

« [L]es pouvoirs et les responsabilités doivent être délégués au niveau approprié d'autorité. Une répartition adéquate des lieux de décision doit être recherchée, en ayant le souci de les rapprocher le plus possible des citoyens et des communautés concernés ».

↳ *– Loi sur le développement durable, art. 6 g) « subsidiarité »*

Responsabilité

- ☐ Un préjudice indu, ou un risque indu de préjudice, ne doit pas être infligé à autrui, que ce soit intentionnellement ou non (**non-malfaisance**).
- ☐ Des mesures suffisantes et raisonnables doivent être prises afin de réduire le plus possible les préjudices et les risques de causer des préjudices (**diligence raisonnable**).
- ☐ Des mises en garde sur les risques encourus par l'usage des données ainsi que des métadonnées de qualité doivent être publiées dans une forme compréhensible et facilement accessible pour favoriser un usage approprié des données, proportionnel à leur nature et à leur qualité (voir ci-dessous le **principe de proportionnalité** s'y rapportant).
- ☐ « [E]n présence d'un risque connu, des actions de prévention, d'atténuation et de correction doivent être mises en place, en priorité à la source ».

  ↳ *– Loi sur le développement durable, art. 6 i) « prévention »*

Proportionnalité des moyens par rapport aux fins

- ☐ Les moyens mis en œuvre doivent être rationnellement liés et proportionnels aux fins qui sont poursuivies.
- ☐ Dès que des données sensibles entrent en jeu, les moyens doivent se limiter à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi, et le moyen qui porte le moins atteinte aux droits et libertés doit être privilégié.
- ☐ Les applications relatives à la sécurité doivent toujours s'accompagner d'une réflexion sur les causes des menaces et sur l'adéquation entre les risques perçus (par les citoyens, par les décideurs politiques) et les risques réels, afin de ne pas reproduire ou renforcer des relations de pouvoir ou des inégalités sociales par le profilage que permettent les technologies numériques.

Proportionnalité de la nature et de la qualité des données par rapport à leurs usages

- ☐ Les moyens mis en œuvre, dont les applications technologiques, doivent être nourris par des données qui sont pertinentes, fiables, complètes et adaptées à l'usage que l'on projette d'en faire.
- ☐ La qualité interne des données – leurs caractéristiques internes et généalogiques, telles que leur actualité, leur exhaustivité et leur source – doit être définie pour déterminer si elles sont aptes à satisfaire les besoins pour lesquels elles sont constituées.

Bien commun

- ☐ La sphère publique est autonome par rapport aux intérêts privés (**autonomie**).
- ☐ Dans les décisions publiques, l'intérêt public prime sur les intérêts privés (**primauté**).
- ☐ La décision publique se fonde sur la conciliation des valeurs, des perspectives et des intérêts pluriels présents dans la société civile et sur la recherche du consensus (**inclusion**).
- ☐ Les projets de ville intelligente doivent entraîner des bénéfices pour la collectivité (**utilité**).
- ☐ Les coûts ne doivent pas être socialisés alors que les bénéfices sont privatisés (**équité**).

Équité

- ☐ Le traitement accordé aux différentes parties doit être juste et impartial, et les disparités en la matière doivent être rigoureusement justifiées en des termes acceptables par tous.
- ☐ Les bénéfices et les inconvénients (dont les coûts) liés à l'innovation doivent être distribués équitablement entre les territoires, ce qui n'implique pas d'aplanir des disparités normales et légitimes telles que celles liées à la densité de population ou à l'accès aux ressources, ou découlant de l'application de principes comme la maximisation des bénéfices collectifs (**justice spatiale**).
- ☐ Une attention particulière doit être portée aux conséquences des projets de ville intelligente sur la fracture numérique, c'est-à-dire sur les inégalités d'accès et d'utilisation liées au numérique et à ses bénéfices qui résultent de diverses conditions matérielles, sociales et cognitives et qui touchent différentes populations, qu'elles soient composées de personnes âgées, précaires, marginalisées, peu scolarisées ou en situation de handicap (**inclusion numérique**).
- ☐ « [L]es actions de développement doivent être entreprises dans un souci d'équité intra et intergénérationnelle ainsi que d'éthique et de solidarité sociales ».

  ↳ *– Loi sur le développement durable, art. 6 b) « équité et solidarité sociales »*

Protection de la vie privée, de la confidentialité et de la sécurité des données sensibles

☐ Le principe de proportionnalité des moyens par rapport aux fins doit être appliqué.

La Loi canadienne sur la protection des renseignements personnels et les documents électroniques énonce une série de principes relatifs à l'équité dans le traitement de l'information. De même, l'OCDE publie les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, qui contiennent aussi des principes fondamentaux. Enfin, le Commissaire à l'information et à la protection de la vie privée de l'Ontario a proposé, dans les années 1990, sept principes de la protection intégrée de la vie privée (PIVP), qui forment un cadre reconnu dans le monde entier en la matière.

La Commission considère que ces ensembles de principes peuvent servir de cadre de référence pour la réflexion sur la modernisation du cadre légal. Les municipalités peuvent aussi se référer à ces principes afin de prévenir les risques juridiques liés à la protection de la vie privée. Ces principes demeurent pertinents, même à la suite des développements technologiques qui posent des défis dans le cadre légal actuel. Leur application doit cependant être repensée au regard des nouvelles situations. Voir l'annexe 4

Appendix C
NYC's Guidelines for Building a Smart + Equitable City

C. NYC's Guidelines for Building a Smart + Equitable City

NYC's Guidelines for Building a Smart + Equitable City were published in 2016 and 30 cities, including Paris, have subsequently signed them.

Principle 1: Privacy and Transparency

City IoT deployments must protect and respect the privacy of residents and visitors. The City is committed to being open and transparent about the "who, what, where, when, why and how" of data collection, transmission, processing and use.

1.1: The City should make processes and policies related to IoT and IoT-related data publicly available in an up-to-date, clear and comprehensive manner. IoT principles, guidelines, operational policies and responsibilities should be transparent and made public via a City government website.

1.2: IoT data should only be collected, transmitted, processed and used for specified, explicit and legitimate purposes. The purpose of data collection (e.g., a use case such as monitoring air quality), what data is collected (e.g., particulates in the air) and how data is being collected (e.g., pollution sensor on a light pole) should be transparent and made public via a City government website or other public notice.

1.3: Data and information collected by IoT devices should be classified and treated accordingly, per the City of New York's Data Classification Policy, as Public, Sensitive, Private or Confidential. All personally identifiable information (PII) should be classified at a minimum as private. All data that is classified as being confidential, or personally identifiable, should be protected from unauthorized use and disclosure (link to New York City Data Classification Policy).

1.4: PII should by default be anonymized before being shared in any way that could make the information publicly searchable or discoverable. Any copies and reproductions must have the same or higher level of classification as the original. Any combinations of data should be reclassified according to the City's Data Classification Policy. (Link to New York City Data Encryption Policy).

1.5: PII data types should have a clearly associated retention policy and disposal procedure. Sensitive, private or confidential data should be kept for no longer than is operationally necessary or required for the specified, explicit and legitimate purposes. (Link to New York City Digital Media Re-use and Disposal Policy).

1.6: Before any sensitive, private, or confidential data is shared outside the originating City agency, the agency should ensure that the need cannot be met by using anonymized or aggregated data and that the appropriate protections are in place to preserve the confidentiality of the data.

1.7: All public data sets are subject to the NYC Open Data Law and as such should be freely accessible via the City's Open-data portal.

Principle 2: Data Management

City IoT deployments must protect and respect the privacy of residents and visitors. The City is committed to being open and transparent about the "who, what, where, when, why and how" of data collection, transmission, processing and use.

2.1: IoT systems (e.g. how data is collected, analyzed and used) should be designed with the use case in mind (e.g. predicting demand for trash pick-up based on data on trash volume, weather and events) to maximize the benefits that can be derived data collection (e.g. routing garbage trucks more efficiently). Where useful, relevant business and historical data from the City or its partners should be made available and utilized by applications.

2.2: The desired measurement from any IoT system (e.g. pedestrian counts) should be collected and categorized as efficiently as possible, using as few steps and/or manipulations as necessary.

2.3: IoT data should be collected and stored according to open standards, contain relevant contextual metadata, be exposed through open, standards-based application program interfaces (APIs), and be provided with software development kits (SDKs) where applicable so it can be easily shared or combined with other data sets.

2.4: IoT data should be archived in a federated way and made accessible throughout the City through a central portal (e.g. the City's open-data portal) or a catalogue of documented open APIs unless restricted by existing laws or regulations and/or doing so would compromise privacy or public safety. Data from other systems not operated by the City, such as from a private sector partner or from crowdsourcing, that could provide public benefit can also be provided in this form with the source documented accordingly.

2.5: The City recognizes the use of distinct and sometimes conflicting non-proprietary international, national, or industry standards for data and technology interfaces. In cases where standards conflict, the one that most closely aligns to the use case will be selected.

2.6: Each IoT device data set (e.g. temperature) should be validated and verified (e.g. through redundancy in data collection and/or historical data) and the resulting master copy clearly labeled before it is used, aggregated and/or released. Data should be versioned so that any updated data can be distinguished from the original and/or master copy. The retention and disposal policies for the master copy should be explicitly defined.

2.7: IoT data should be both audited and continuously monitored for accuracy and validity. This process should be automated where possible.

2.8: All data sets (e.g. 311 service requests) should be checked for geographic, social or system-driven bias (e.g. geographic differences in civic engagement) and other quality problems. Any biasing factors should be recorded and provided with the data set and corrected where possible.

Principle 3: Infrastructure

IoT devices, networks and infrastructure shall be deployed, used, maintained and disposed of in an efficient, responsible and secure manner to maximize public benefit.

3.1: To support citywide coordination of IoT deployments, City agencies should maintain an inventory of IoT devices that they deploy using a standardized format. City agencies should also maintain an inventory of the public or private assets on which devices are installed and the networks used by these IoT devices including details on the network type (e.g. LTE), security protocol (e.g. WPA), location, service level agreements, and contact information for the network and system operator.

3.2: The City should accumulate and publish, via a City government website, public information on IoT systems including but not limited to examples of deployed IoT devices (e.g. air quality sensors) and the different types of public assets (e.g. light poles) on which they are deployed.

3.3: The City should make public, via a City government website, a standardized protocol, including points of contact, for requesting access to, and approving use of, City assets for IoT deployments. Where appropriate, the City will detail restrictions on particular types of public assets and/or siting restrictions (e.g. rules for landmark or historic districts).

3.4: IoT deployments shall, where possible, leverage or repurpose existing conduit and public assets, maximize energy efficiency, and adhere to sustainable device disposal procedures.

3.5: The City should leverage existing wireless and fixed networks where possible and appropriate. Networks for IoT deployments should be selected to best support the specific use case. This should include but is not limited to ensuring appropriate security protocols, bandwidth, pricing models, and service level agreements (SLAs).

3.6: All IoT devices and network equipment installed by the City, on the City's behalf, or on City property should have clear site license agreements and established terms of service governing who is responsible for ongoing operations, maintenance, and the secure disposal of equipment. IoT devices and network equipment should be labeled clearly with the name and contact information for the responsible party.

3.7: Public assets should be instrumented in an orderly manner that minimizes clutter and allows for ease of access for replacement, repair and addition of new equipment or devices. If new conduit is being installed using public assets (e.g. to access rooftop of public buildings) or using public right-of-way (e.g. in City streets), location details must be filed with the responsible agency and use of the conduit should not be restricted to one party.

3.8: IoT systems should be designed to maximize resiliency in the event of a natural disaster (e.g. severe flooding) or other emergencies (e.g. electrical outages). Critical systems should have established emergency response plans to ensure the appropriate continuity of service.

Principle 4: Security

IoT systems should be designed and operated with security in mind to protect of the public, ensure the integrity of services, and be resilient to attacks.

4.1: IoT systems should be designed with an explicit focus on minimizing security risks (e.g. unauthorized operation or hacking, system faults, tampering, and environmental risks), limiting the potential impact from a security breach (e.g. the release of personally identifiable information), and ensuring that any compromises can be quickly detected and managed.

4.2: IoT systems should utilize established security frameworks, where possible, and ensure communication between components is tightly constrained.

4.3: Identity and access management controls should be in place to ensure that the right people have access to systems, networks, and data at the right time. Users with access to IoT systems should be identified and authenticated. Identification should be to the individual and not to the role.

4.4: All data should be protected in transit and at rest, and systems should be secured against unauthorized access or operation. Data storage mechanisms must not be easily removed from devices and systems must not have vulnerable external interfaces (e.g. unsecured USB ports).

4.5: All partners utilizing public assets and/or networks for IoT deployments should adhere to the principles and guidelines set by the City. The City has the right to restrict or revoke access to assets, devices, and public networks to protect the public interest and public safety.

4.6: The City and its partners should engage in both audit-based and continuous monitoring to ensure that systems are working and that devices have not been compromised.

4.7: Responsibilities related to security monitoring and the protection of IoT systems should be clearly defined. In the event of a breach, public and private sector entities will be required to comply with the City's breach disclosure and notification requirements.

Principle 5: Operations and Sustainability

All IoT deployments should be structured to maximize public benefit and ensure financial, operational, and environmental sustainability.

5.1: Demonstrated need, business case, and public benefit (e.g. economic, social, and environmental outcomes) should be required prior to deployment of any new IoT devices or solutions. In addition, proof of concept should be required prior to citywide deployments.

5.2: Prior to deployment, the City and its partners shall identify all stakeholder and user groups (e.g. community residents and city employees) that will be impacted by IoT solution and establish feedback mechanisms and methods of engagement for these groups. Before and during deployment, the City and its partners should also check for and address biases in IoT solution (e.g. information asymmetries) that may result in unintended consequences (e.g. inequitable service delivery).

5.3: The City shall prioritize access to its assets and public networks for IoT device deployments that are distributed in an equitable manner and have the greatest public benefit. Public-private partnerships and business models that offset costs or generate revenue in ways aligned with greatest public benefit are encouraged but must be closely evaluated for risk.

5.4: All projects and associated contracts or agreements should outline the "who, what, where, when, why and how" of the implementation, operations, risk management, knowledge transfer, and maintenance of IoT systems. This should include clear definitions related to system and data ownership and responsibilities.

5.5: Solutions shall be designed to be flexible and responsive to evolving needs. Agreements should enable the addition of new functions and update of components over the life of the agreement at a fair and transparent cost.

5.6: Performance metrics should be maintained for solutions. Agreements should specify intended outcomes of a solution and levels of service and provide for penalties, modifications, or terminations of the agreement in the event that the solution does not perform.

5.7: The City and its partners should reuse infrastructures and components where possible, leverage citywide contracts or agreements, and develop solutions collaboratively among agencies to avoid duplicating existing solutions or functions and extract the greatest value from investments.

5.8: All components of a solution should be implemented in a modular manner, prioritizing open standards where possible, to ensure interoperability and prevent dependency on a single vendor.

Appendix D
Asilomar AI PRINCIPLES

D. Asilomar AI Principles

Research Issues

1) **Research Goal:** The goal of AI research should be to create not undirected intelligence, but beneficial intelligence.

2) **Research Funding:** Investments in AI should be accompanied by funding for research on ensuring its beneficial use, including thorny questions in computer science, economics, law, ethics, and social studies, such as:

- How can we make future AI systems highly robust, so that they do what we want without malfunctioning or getting hacked?
- How can we grow our prosperity through automation while maintaining people's resources and purpose?
- How can we update our legal systems to be more fair and efficient, to keep pace with AI, and to manage the risks associated with AI?
- What set of values should AI be aligned with, and what legal and ethical status should it have?

3) **Science-Policy Link:** There should be constructive and healthy exchange between AI researchers and policy-makers.

4) **Research Culture:** A culture of cooperation, trust, and transparency should be fostered among researchers and developers of AI.

5) **Race Avoidance:** Teams developing AI systems should actively cooperate to avoid corner-cutting on safety standards.

Ethics and Values

6) **Safety:** AI systems should be safe and secure throughout their operational lifetime, and verifiably so where applicable and feasible.

7) **Failure Transparency:** If an AI system causes harm, it should be possible to ascertain why.

8) **Judicial Transparency:** Any involvement by an autonomous system in judicial decision-making should provide a satisfactory explanation auditable by a competent human authority.

9) **Responsibility:** Designers and builders of advanced AI systems are stakeholders in the moral implications of their use, misuse, and actions, with a responsibility and opportunity to shape those implications.

10) **Value Alignment:** Highly autonomous AI systems should be designed so that their goals and behaviors can be assured to align with human values throughout their operation.

11) **Human Values:** AI systems should be designed and operated so as to be compatible with ideals of human dignity, rights, freedoms, and cultural diversity.

12) **Personal Privacy:** People should have the right to access, manage and control the data they generate, given AI systems' power to analyze and utilize that data.

13) **Liberty and Privacy:** The application of AI to personal data must not unreasonably curtail people's real or perceived liberty.

14) **Shared Benefit:** AI technologies should benefit and empower as many people as possible.

15) **Shared Prosperity:** The economic prosperity created by AI should be shared broadly, to benefit all of humanity.

16) **Human Control:** Humans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.

17) **Non-subversion:** The power conferred by control of highly advanced AI systems should respect and improve, rather than subvert, the social and civic processes on which the health of society depends.

18) **AI Arms Race:** An arms race in lethal autonomous weapons should be avoided.

Longer-term Issues

19) **Capability Caution:** There being no consensus, we should avoid strong assumptions regarding upper limits on future AI capabilities.

20) **Importance:** Advanced AI could represent a profound change in the history of life on Earth, and should be planned for and managed with commensurate care and resources.

21) **Risks:** Risks posed by AI systems, especially catastrophic or existential risks, must be subject to planning and mitigation efforts commensurate with their expected impact.

22) **Recursive Self-Improvement:** AI systems designed to recursively self-improve or self-replicate in a manner that could lead to rapidly increasing quality or quantity must be subject to strict safety and control measures.

23) **Common Good:** Superintelligence should only be developed in the service of widely shared ethical ideals, and for the benefit of all humanity rather than one state or organization.

Appendix E
Montréal Declaration

E. *Montréal Declaration*

PREAMBLE

Intelligence, whether it be natural or artificial, has no value in and of itself. An individual's intelligence does not tell us anything about his or her morality; this is also the case for any other intelligent entity. Intelligence can, however, have an instrumental value: it is a tool that can lead us away from or towards a goal we wish to attain. Thus, artificial intelligence can create new risks and exacerbate social and economic inequalities. But it can also contribute to well-being, freedom and justice.

From an ethical point of view, the development of AI poses previously unknown challenges. For the first time in history, we have the opportunity to create non-human, autonomous and intelligent agents that do not need their creators to accomplish tasks that were previously reserved for the human mind. These intelligent machines do not merely calculate better than human beings, they also look for, process and disseminate information. They interact with sentient beings, human or non-human. Soon, they will even be able to keep them company, as would a parent or a friend.

These artificial agents will come to directly influence our lives. In the long term, we could create "moral machines," machines able to make decisions according to ethical principles. We must ask ourselves if these developments are responsible and desired. And we can hope that AI will make our societies better, in the best interest of, and with respect for, everyone.

The principles and recommendations that we are asking you to develop collectively are ethical guidelines for the development of artificial intelligence. In this first phase of the declaration, we have identified seven values: well-being, autonomy, justice, personal privacy, knowledge, democracy and responsibility. For each value, you will find a series of questions that seek to explore its relationship with the development of AI. We then put forth a normative principle, one that does not directly answer the questions asked.

VALUES, QUESTIONS, PRINCIPLES

Well-being

- How can AI contribute to personal well-being?
- Is it acceptable for an autonomous weapon to kill a human being? What about an animal?
- Is it acceptable for AI to control the running of an abattoir?
- Should we entrust AI with the management of a lake, a forest or the Earth's atmosphere?
- Should we develop AI technology which is able to sense a person's well-being?

Proposed principle:
The development of AI should ultimately promote the well-being of all sentient creatures.

Autonomy
- How can AI contribute to greater autonomy for human beings?
- Must we fight against the phenomenon of attention-seeking which has accompanied advances in AI?
- Should we be worried that humans prefer the company of AI to that of other humans or animals?
- Can someone give informed consent when faced with increasingly complex autonomous technologies?
- Must we limit the autonomy of intelligent computer systems? Should a human always make the final decision?

Proposed principle:
The development of AI should promote the autonomy of all human beings and control, in a responsible way, the autonomy of computer systems.

Justice
- How do we ensure that the benefits of AI are available to everyone?
- Must we fight against the concentration of power and wealth in the hands of a small number of AI companies?
- What types of discrimination could AI create or exacerbate?
- Should the development of AI be neutral or should it seek to reduce social and economic inequalities?
- What types of legal decisions can we delegate to AI?

Proposed principle:
The development of AI should promote justice and seek to eliminate all types of discrimination, notably those linked to gender, age, mental / physical abilities, sexual orientation, ethnic / social origins and religious beliefs.

Privacy
- How can AI guarantee respect for personal privacy?
- Do our personal data belong to us and should we have the right to delete them?
- Should we know with whom our personal data are shared and, more generally, who is using these data?
- Does it contravene ethical guidelines or social etiquette for AI to answer our e-mails for us?
- What else could AI do in our name?

Proposed principle:
The development of AI should offer guarantees respecting personal privacy and allowing people who use it to access their personal data as well as the kinds of information that any algorithm might use.

Knowledge

- Does the development of AI put critical thinking at risk?
- How do we minimize the dissemination of fake news or misleading information?
- Should research results on AI, whether positive or negative, be made available and accessible?
- Is it acceptable not to be informed that medical or legal advice has been given by a chatbot?
- How transparent should the internal decision-making processes of algorithms be?

Proposed principle:
The development of AI should promote critical thinking and protect us from propaganda and manipulation.

Democracy

- How should AI research and its applications, at the institutional level, be controlled?
- In what areas would this be most pertinent?
- Who should decide, and according to which modalities, the norms and moral values determining this control?
- Who should establish ethical guidelines for self-driving cars?
- Should ethical labeling that respects certain standards be developed for AI, websites and businesses?

Proposed principle:
The development of AI should promote informed participation in public life, cooperation and democratic debate.

Responsibility

- Who is responsible for the consequences of the development of AI?
- How should we define progressive or conservative development of AI?
- How should we react when faced with AI's predictable consequences on the labour market?
- Is it acceptable to entrust a vulnerable person to the care of AI (for example, a "robot nanny")?
- Can an artificial agent, such as Tay, Microsoft's "racist" chatbot, be morally culpable and responsible?

Proposed principle:
The various players in the development of AI should assume their responsibility by working against the risks arising from their technological innovations.

DEFINITIONS

Sentient being
Any being able to feel pleasure, pain, emotions; basically, to feel. At the current state of scientific knowledge, all vertebrates and some invertebrates such as octopi, are considered sentient beings. In biology, the development of this characteristic can be explained by the theory of evolution.

Ethics (or Morals)
This is the discipline that ponders the proper ways to behave, individually or collectively, by looking to adopt an impartial point of view. It is based on moral norms and values.

Moral values
Moral values are related to good and evil: they allow us, for example, to qualify an action as just or unjust, honest or dishonest, commendable or blameworthy.

Epistemic value
Epistemic values are related to knowledge: they allow us, for example, to qualify an argument as valid or invalid, clear or unclear, pertinent or trivial.

Intrinsic value
A value is intrinsic when it is an ultimate justification, when one looks for it in and of itself. For example, well-being, autonomy and justice can be looked in and of themselves; thus they are intrinsic values.

Instrumental value
A value is instrumental when it is in service of something else, when it helps promote an intrinsic value, for example. Money and intelligence are examples of instrumental values that can be put to the service of well-being, autonomy or justice.

Utopia
A possible world which embodies a collection of positive values. Thus, it can be said that a society in which AI frees people from all unpleasant work, allowing them to take care of each other while fully developing their personal potential, would be a utopian society.

Dystopia

This is the opposite of a utopia. It is a possible world that embodies a collection of negative values. Thus, it can be said that a society in which several corporations (or a single corporation) become extremely powerful thanks to AI, allowing them to control and exploit people, would be a dystopian society.

Appendix F
ACM Code of Ethics (2018)

F. 2018 ACM Code of Ethics and Professional Conduct: Draft 2

Draft 2 was developed by The Code 2018 Task Force.

(It is based on the 2018 *ACM Code of Ethics and Professional Conduct*: Draft 1)

Preamble

The ACM Code of Ethics and Professional Conduct ("the Code") identifies key elements of ethical conduct in computing.

The Code is designed to support all computing professionals, which is taken to mean current or aspiring computing practitioners as well as those who influence their professional development, and those who use technology in an impactful way. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always a primary consideration. Section 1 outlines fundamental ethical considerations. Section 2 addresses additional, more specific considerations of professional responsibility. Section 3 pertains more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member and principles involving compliance with the Code are given in Section 4.

The Code as a whole is concerned with how fundamental ethical principles apply to one's conduct as a computing professional. Each principle is supplemented by guidelines, which provide explanations to assist members in understanding and applying it. These extraordinary ethical responsibilities of computing professionals are derived from broadly accepted ethical principles.

The Code is not an algorithm for solving ethical problems, rather it is intended to serve as a basis for ethical decision making in the conduct of professional work. Words and phrases in a code of ethics are subject to varying interpretations, and a particular principle may seem to conflict with other principles in specific situations. Questions related to these kinds of conflicts can best be answered by thoughtful consideration of the fundamental ethical principles, understanding the public good is the paramount consideration. The entire profession benefits when the ethical decision making process is transparent to all stakeholders. In addition, it may serve as a basis for judging the merit of a formal complaint pertaining to a violation of professional ethical standards.

1. GENERAL MORAL PRINCIPLES

A computing professional should…

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect diversity. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. Computing professionals should give consideration to whether the products of their efforts will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work. When the interests of multiple groups conflict the needs of the least advantaged should be given increased attention and priority.

In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should be alert to, and make others aware of, any potential harm to the local or global environment.

1.2 Avoid harm.

In this document, "harm" means negative consequences to any stakeholder, especially when those consequences are significant and unjust. Examples of harm include unjustified death, unjustified loss of information, and unjustified damage to property, reputation, or the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may unexpectedly lead to harm. In such an event, those responsible are obligated to undo or mitigate the harm as much as possible. Avoiding unintentional harm begins with careful consideration of potential impacts on all those affected by decisions.

To minimize the possibility of indirectly harming others, computing professionals should follow generally accepted best practices for system design, development, and testing. Additionally, the consequences of emergent systems and data aggregation should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

At work, a computing professional has an additional obligation to report any signs of system risks that might result in serious personal or social harm. If one's superiors do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, the computing professional should thoroughly assess all relevant aspects of the incident as outlined in Principle 2.5.

1.3 Be honest and trustworthy.

Honesty is an essential component of trust. A computing professional should be fair and not make deliberately false or misleading claims and should provide full disclosure of all pertinent system limitations and potential problems. Fabrication of data, falsification of data, and scientific misconduct are similarly violations of the Code. One who is professionally dishonest is accountable for any resulting harm.

A computing professional should be honest about his or her own qualifications, and about any limitations in competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to conflicts of interest or otherwise tend to undermine the independence of their judgment.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member should exercise care not to misrepresent ACM, or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate.

The values of equality, tolerance, respect for others, and equal justice govern this principle. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of ACM policy. Sexual harassment is a form of discrimination that limits fair access to the spaces where the harassment takes place.

Inequities between different groups of people may result from the use or misuse of information and technology. Technologies should be as inclusive and accessible as possible. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

1.5 Respect the work required to produce new ideas, inventions, and other creative and computing artifacts.

The development of new ideas, inventions, and other creative and computing artifacts creates value for society, and those who expend the effort needed for this should expect to gain value from their work. Computing professionals should therefore provide appropriate credit to the creators of ideas or work. This may be in the form of respecting authorship, copyrights, patents, trade secrets, non-disclosure agreements, license agreements, or other methods of attributing credit where it is due.

Both custom and the law recognize that some exceptions to a creator's control of a work are necessary to facilitate the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works.

Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and other work put into the public domain. Computing professionals should avoid misappropriation of a commons.

1.6 Respect privacy.

"Privacy" is a multi-faceted concept and a computing professional should become conversant in its various definitions and forms.

Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Computing professionals should use personal data only for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals or groups. Computing professionals should establish procedures that allow individuals to review their personal data, correct inaccuracies, and opt out of automatic data collection.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined and enforced, and personal information gathered for a specific purpose should not be used for other purposes without consent of the individual(s). When data collections are merged, computing professionals should take special care for privacy. Individuals may be readily identifiable when several data collections are merged, even though those individuals are not identifiable in any one of those collections in isolation.

1.7 Honor confidentiality.

Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code.

User data observed during the normal duties of system operation and maintenance should be treated with strict confidentiality, except in cases where it is evidence for the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities, and the computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

2. PROFESSIONAL RESPONSIBILITIES

A practicing computing professional should…

2.1 Strive to achieve the highest quality in both the process and products of professional work.

Computing professionals should insist on high quality work from themselves and from colleagues. This includes respecting the dignity of employers, colleagues, clients, users, and anyone affected either directly or indirectly by the work. High quality process includes an obligation to keep the client or employer properly informed about progress toward completing that project. Professionals should be cognizant of the serious negative consequences that may result from poor quality and should resist any inducements to neglect this responsibility.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

High quality computing depends on individuals and teams who take personal and organizational responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and awareness of the social context in which the work may be deployed. Professional competence also requires skill in reflective analysis for recognizing and navigating ethical challenges. Upgrading necessary skills should be ongoing and should include independent study, conferences, seminars, and other informal or formal education. Professional organizations, including ACM, are committed to encouraging and facilitating those activities.

2.3 Know, respect, and apply existing laws pertaining to professional work.

ACM members must obey existing regional, national, and international laws unless there is a compelling ethical justification not to do so. Policies and procedures of the organizations in which one participates must also be obeyed, but compliance must be balanced with the recognition that sometimes existing laws and rules are immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review.

Quality professional work in computing depends on professional reviewing and critiquing. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.

Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computing professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. Extraordinary care should be taken to identify and

mitigate potential risks in self-changing systems. Systems whose future risks are unpredictable require frequent reassessment of risk as the system develops or should not be deployed. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in Principle 1.3.

As noted in the guidance for Principle 1.2 on avoiding harm, any signs of danger from systems should be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for Principle 1.2 for more details concerning harm, including the reporting of professional violations.

2.6 Accept only those responsibilities for which you have or can obtain the necessary expertise, and honor those commitments.

A computing professional has a responsibility to evaluate every potential work assignment. If the professional's evaluation reveals that the project is infeasible, or should not be attempted for other reasons, then the professional should disclose this to the employer or client, and decline to attempt the assignment in its current form.

Once it is decided that a project is feasible and advisable, the professional should make a judgment about whether the project is appropriate to the professional's expertise. If the professional does not currently have the expertise necessary to complete the project the professional should disclose this shortcoming to the employer or client. The client or employer may decide to pursue the project with the professional after time for additional training, to pursue the project with someone else who has the required expertise, or to forego the project.

The major underlying principle here is the obligation to accept personal accountability for professional work. The computing professional's ethical judgment should be the final guide in deciding whether to proceed.

2.7 Improve public understanding of computing, related technologies, and their consequences.

Computing professionals have a responsibility to share technical knowledge with the public by creating awareness and encouraging understanding of computing, including the impacts of computer systems, their limitations, their vulnerabilities, and opportunities that they present. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so.

This principle derives from Principle 1.2–"Avoid harm to others." No one should access or use another's computer system, software, or data without permission. One should have appropriate approval before using system resources, unless there is an overriding concern for the public good. To support this clause, a computing professional should take appropriate action to secure resources against unauthorized use. Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code (such as Principle 1.4).

3. PROFESSIONAL LEADERSHIP PRINCIPLES

In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. These principles generally apply to organizations and groups, as well as their leaders.

A computing professional acting as a leader should…

3.1 Ensure that the public good is a central concern during all professional computing work.

The needs of people—including users, other people affected directly and indirectly, customers, and colleagues—should always be a central concern in professional computing. Tasks associated with requirements, design, development, testing, validation, deployment, maintenance, end-of-life processes,

and disposal should have the public good as an explicit criterion for quality. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of the social responsibilities of members of an organization or group.

Technical organizations and groups affect the public at large, and their leaders should accept responsibilities to society. Organizational procedures and attitudes oriented toward quality, transparency, and the welfare of society will reduce harm to members of the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation in meeting social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to design and build systems that enhance the quality of working life.

Leaders are responsible for ensuring that systems enhance, not degrade, the quality of working life. When implementing a system, leaders should consider the personal and professional development, accessibility, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.4 Establish appropriate rules for authorized uses of an organization's computing and communication resources and of the information they contain.

Leaders should clearly define appropriate and inappropriate uses of organizational computing resources. These rules should be clearly and effectively communicated to those using their computing resources. In addition, leaders should enforce those rules, and take appropriate action when they are violated.

3.5 Articulate, apply, and support policies that protect the dignity of users and others affected by computing systems and related technologies.

Dignity is the principle that all humans are due respect. This includes the general public's right to autonomy in day-to-day decisions.

Designing or implementing systems that deliberately or inadvertently violate, or tend to enable the violation of, the dignity or autonomy of individuals or groups is ethically unacceptable. Leaders should verify that systems are designed and implemented to protect dignity.

3.6 Create opportunities for members of the organization and group to learn, respect, and be accountable for the principles, limitations, and impacts of systems.

This principle complements Principle 2.7 on public understanding. Educational opportunities are essential to facilitate optimal participation of all organization or group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties, including experiences that familiarize them with the consequences and limitations of particular types of systems. Professionals should know the dangers of oversimplified models, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and the contexts in which they are deployed, and other issues related to the complexity of their profession.

3.7 Recognize when computer systems are becoming integrated into the infrastructure of society, and adopt an appropriate standard of care for those systems and their users.

Organizations and groups occasionally develop systems that become an important part of the infrastructure of society. Their leaders have a responsibility to be good stewards of that commons. Part of that stewardship requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, there are likely to be changes in the

ethical responsibilities of the organization. Leaders of important infrastructure services should provide due process with regard to access to these services. Continual monitoring of how society is using a product will allow the organization to remain consistent with their ethical obligations outlined in the principles of the code. Where such standards of care do not exist, there may be a duty to develop them.

4. COMPLIANCE WITH THE CODE

A computing professional should…

4.1 Uphold, promote, and respect the principles of the Code.

The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles expressed in the Code. Each ACM member should encourage and support adherence by all computing professionals. Computing professionals who recognize breaches of the Code should take whatever actions are within their power to resolve the ethical issues they recognize.

4.2 Treat violations of the Code as inconsistent with membership in ACM.

If an ACM member does not follow the Code, membership in ACM may be terminated.

Appendix G
List of General and Specific Principles

This appendix partially appears below and is found in the first tab of the Excel file *Compilation finale principles 10 12 2017*

G. Final List of Principles

Valeurs et principes	Principes spécifiques	Autres principes spécifiques
Bien commun		
Assurer que l'IDO soit au service du bien commun et de la démocratie (inspiré de CÉSTQ)		
	Le projet de l'IdO doit entraîner des bénéfices pour la collectivité (CÉSTQ) (inspiré Asilomar, FAPPs)	
	Le projet de l'IdO doit se fonder sur la conciliation des valeurs, perspectives, intérêts pluriels présents dans la société civile et sur la recherche de	
	Le projet de l'IdO doit être proportionnel aux objectifs visés (CÉSTQ)	
	Les coûts ne doivent pas être socialisés alors que les bénéfices sont privatisés (équité)(CÉSTQ)	
	Le projet de l'IdO doit viser l'optimum social - pas seulement l'optimisation des services/processus - FORMULATION BASÉE SUR LES ENJEUX ID. DA	
	Les preneurs de décisions municipaux doivent être conscients des angles morts existant dans les données et projets (ex: amélioration des service	
	Le projet de l'IdO doit contribuer à la cohésion sociale, plutôt que l'individualisation de la ville - FORMULATION BASÉE SUR LES ENJEUX ID. DANS F	
Démocratie et participation citoyenne		
Promouvoir la participation citoyenne pour définir une vision concertée du projet de l'IdO et s'assurer que celui-ci soit l'objet de délibération démocratique (inspiré d		
	La participation et l'engagement des citoyens et des groupes qui les représentent sont nécessaires pour définir une vision concertée (CÉSTQ)	
	Le projet de l'IdO doit contribuer à améliorer les pratiques démocratiques, mais aussi être objet de la délibération démocratique (CÉSTQ, FAPPs -	
	Droit à soustraire ses données: Donner aux citoyens la possibilité de soustraire leurs données lorsque possible (Seattle, Euro 2018)	
	Débattre des décisions éthiques difficiles: plutôt que de les voir comme des problèmes, l'absence de solutions évidentes et protocoles de gouver	
	Toute décision émanant du projet de l'IdO doit être rattachée à responsabilité décisionnelle humaine - FORMULATION BASÉE SUR LES ENJEUX ID.	
La vie privée		
Protéger et respecter la vie privée des citoyens		
	Détermination des fins de la collecte: Informer le sujet des informations collectées et de la finalité de la collecte avant ou lors de la collecte (Norr	
	Consentement: Les informations doivent être collectées avec le consentement des individus (Normes Canada - FIPPs, OCDE, ACM)	
	Limitation de la collecte: L'organisation ne peut recueillir que les informations nécessaires aux fins déterminées et doit procéder de façon honnêt	
	Utilisation pour les fins annoncées: Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxq	
	Durée de vie des données: On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins dé	
	Qualité de données: Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés	
	Vie privée par défaut: Respecter la vie privée comme paramètre par défaut - automatique protégé (Ontario, VPDC)	
		Anonymisation: les renseignements personnels devraient être anonymisés par défaut avant de rendre l'information publiq
		Éviter la réidentification des données: notamment en identifiant les possibles vecteurs de réidentification des données
		Favoriser les informations ouvertes anonymisées et agrégées (Lignes IdO)
		Vie privée dans un environnement de données massives: Lorsque des bases de données sont croisées, considérer les perte
		Les tierces parties sous-contractées ayant accès aux données personnelles devront se soumettre à la politique de la vie pri
	Vie privée dès la conception (Ontario, VPDC)	
	*Formulation potentiellement utile: Recognize that privacy is more than a binary value: privacy is contextual [11] and situational [12], not reduct	
Transparence		
Être transparent sur le « qui, quoi, quand, où, pourquoi et comment » de la collecte, la transmission, le traitement et l'utilisation (Lignes IdO)		
	Transparence de la gestion: Transparence des politiques et pratiques concernant la gestion de l'information (Normes Canada)	
	Transparence de l'identité du maître du fichier et le siège habituel de ses activités (FIPPs)	
	Transparence sur données détenues et transférées: Informer sujets des infos détenues à son sujet et communiquées à des tiers (Normes Canada	
	Transparence sur l'utilisation des données (FIPPs)	
	Recours possible pour contester l'exactitude des renseignements avec correction possible (Normes Canada - adaptation)	
	*Formulation intéressante: La ville s'engage à être ouverte et transparente par rapport au « qui, quoi, où, pourquoi et comment » de la collecte	
Sécurité		
Concevoir et opérer le système IdO en toute sécurité afin de protéger le public, assurer l'intégrité des services et être résilient face aux attaques (Lignes IdO)		
	Système sécurisé: Le système IdO devrait être conçu avec l'intention de minimiser les risques de sécurité, limiter l'impact d'une brèche de sécurit	
	Renseignements personnels sécurisés: Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à	
	Notification en cas de fuites de données (Euro 2018 - et aussi FTC (de mémoire))	
	Défaillances transparentes: Les défaillances des systèmes automatisés ne devraient pas être surprenantes, silencieuses ou irrésolubles.(FAPPs)	
	Prédictibilité : Les systèmes automatisés devraient être initialement et continuellement inventoriés pour des comportements prédictibles et impr	
	*À ajouter: les mesures dans le principe 4 "Security" dans les Lignes directrices ville intelligente et équitable (Lignes IdO)	

Bonne gestion des données	
Les systèmes devraient être conçus en ayant leur utilisation en tête, pour en maximiser les bénéfices (Lignes IdO)	
	*À ajouter: les mesures dans le principe 2 "Data management" dans les Lignes directrices ville intelligente et équitable (Lignes IdO)
Évaluer et comprendre les conséquences	
Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données et veiller à l'analyse des conséquences à long terme sur les valeur	
	Réaliser des évaluations d'impact sur enjeux éthiques pour tous nouveaux programmes de données (Seattle)
	Les systèmes automatisés ne devraient pas être déployés sans une évaluation des risques pour l'humain dans la boucle (human in the loop) ou les
	Comprendre les perceptions et craintes de la population montréalaise par rapport au projet de l'IdO - FORMULATION BASÉE SUR LES ENJEUX ID. D
	Veiller à l'analyse des conséquences à long terme du projet de l'IdO sur les valeurs sociales élargies (FAPPs) et sur l'environnement, en particulier
Inclusion et non discrimination	
Mettre tous les moyens en œuvre pour éviter le profilage, la discrimination et pour développer un projet inclusif (CÉSTQ)	
	Application relatives à la sécurité doivent s'accompagner d'un réflexion sur les possibilités de profilage et discrimination (...) (CÉSTQ, inspiré ACM)
	Une attention particulière doit être portée aux conséquences des projets de ville intelligente sur la fracture numérique - les inégalités d'accès et d
	Considérer l'effet de la fracture numérique sur les données et les représentations émanant du projet de l'IdO (inspiré de CÉSTQ)
	Diversité et discrimination : Les systèmes automatisés devraient réfléchir sur les biais et les choix durant le design et tester les impacts discriminat
	Les bénéfices et les inconvénients liés à l'innovation doivent être distribués équitablement entre les territoires (CÉSTQ)
Autonomie des pouvoirs publics	
Assurer l'autonomie de la sphère publique et la primauté de l'intérêt public par rapport aux intérêts privés (CÉSTQ)	
	La sphère publique est autonome par rapport aux intérêts privés (autonomie) (CÉSTQ)
	Dans les décisions publiques, l'intérêt public prime sur les intérêts privés (primauté) (CÉSTQ)
Explicabilité des systèmes	
Concevoir des systèmes auditables et dans des cas de prise de décision automatisée, donner aux individus accès aux logiques qui président dans la décision	
	Pour toute décision individuelle automatisée l'individu a le droit de connaître la logique impliquée dans la décision (Euro 1990).
	Pour tout système IA qui provoque un tort (*harm*), il devrait être possible d'expliquer pourquoi (Asilomar)
	Les systèmes automatisés devraient être compréhensibles et supporter la connaissance situationnelle, via une transparence. (FAPPs)
	Concevoir systèmes pour qu'ils soient auditables (FAPPs)
	S'impliquer dans l'analyse des conséquences plus larges des pratiques de collecte et analyse des données (10 règles)
Liberté	
Assurer que le citoyen puisse préserver son sentiment de liberté - FORMULATION BASÉE SUR LES ENJEUX ID. DANS REVUE DE LITTÉRATURE	
	Assurer que le citoyen ne fasse pas constamment l'objet de suivi dans sa vie quotidienne et l'informer du suivi effectué - FORMULATION BASÉE SU
	Assurer que le citoyen ait pleinement le choix de ne pas dépendre d'analyses prédictives qui orientent ses choix - FORMULATION BASÉE SUR LES E
	Assurer que les situations dans lesquelles l'accès des citoyens soit décidé par le biais d'analyses perscriptives soient limités, documentés de façon