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

February 2018

Prepared for

Ville de Montréal

To the attention of Mr. Jean-Martin Thibault
Director (CTO), IT Architecture, Innovation and Security
Ville de Montréal
275, rue Notre-Dame Est
Montréal, QC, HCY 1C6
Canada

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.

DISCLAIMER

The authors are responsible for the selection and presentation of their findings. The opinions expressed in this document are those of the project team and do not necessarily reflect the views of CIRAIG, Polytechnique Montréal or ESG-UQÀM.

With the exception of documents produced by CIRAIG (such as this report), any use of the name of CIRAIG, Polytechnique Montréal or ESG-UQÀM in public disclosures relating to this report must receive prior written consent from a duly appointed representative of CIRAIG, Polytechnique Montréal or ESG-UQÀM.

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

Working Group

Research Team

Execution

Sara Russo Garrido
Supervision, Research and Writing

Marie-Claude Allard
Research and Writing

Joanie Béland
Research and Writing

Emmanuelle Caccamo
Research and Writing

Tyler Reigeluth
Research and Writing

Jean-Philippe Agaisse
Research and Writing

Marie-Luc Arpin
Editing

Project Administration

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 and Martin-Guy Richard.

Summary

Introduction

Since 2014, Montréal has been implementing a strategic initiative to become an internationally renowned leader among smart and digital cities. Montréal plans to develop on its own—and in partnership with residents—technological solutions to the metropolis's key challenges, which it will deploy transparently, with advanced technologies and on a human scale (Ville de Montréal, 2017).

Installation of technological infrastructure is central to the deployment strategy, which includes the development of the city's Internet of Things (IoT), accompanied by the creation of a technological and analytical data collection, storage and analysis system. IoT also means installing a multitude of sensors around the city to gather a wide variety of data on assets and activities throughout the metropolis. One of this digital strategy's key features is the collection of data from sensors and external sources for internal use by the city and its partners, along with external use through big data releases.

While the exploitation of data acquired through IoT offers opportunities to innovate and improve Montreal's quality of life, it raises ethical issues and risks that could trigger social opposition.

Like the advent of urban verticality[1] in the late 20th century and the creation of a highway system in the 1930s, IoT represents a reboot of the urban structure—one built around the convergence arising from Economy 4.0.[2] This transformation of urban architecture is not only the outgrowth of technological evolution, but a driving force in social change.

This report outlines potential issues of ethics and social acceptability pertaining to urban IoT and identifies potential solutions, to support the city in its deliberations on this topic. This document also serves as a stepping-stone to subsequent project phases, such as finding a conceptual framework for developing a program to study, manage and address issues of ethics and social acceptability with respect to the IoT project.

[1] The emergence of high rises, with people living one floor over the other, has given rise to unprecedented population densities.

[2] The "4.0 Economy" emerged out of the fourth industrial revolution. While the third industrial revolution made electronics and IT central to society, the fourth is characterized by a merger of technologies that blur boundaries between the physical, digital and biological spheres. Algorithmic analysis, the Internet of Things and big data are core technological components of the 4.0 Economy (Schwab, 2017).

Basic Concepts: Ethical Issues and Social Acceptability

Ethical issues are identified in this report whenever a basic value or moral principle comes into play in a particular matter or situation (Commission de l'éthique en science et technologie du Québec, 2017). As we know, ethics is a statement of the core values and principles that should guide and direct our interactions with others. These values and principles give meaning to our lives and enable us to distinguish, in a given context, between good/evil, right/wrong, and appropriate/inappropriate.[3]

"Social acceptability" is a controversial term, which has been the subject of numerous debates over its definition (Gendron, 2014; Battelier, 2015). For this project, we shall use Gendron's definition of social acceptability (2014) as "the public sentiment that a plan or decision resulting from collective wisdom is better than known alternatives, including the status quo."

IoT Technological and Analytical Flowchart

Our review of the literature is designed to cover all topics relevant to the specific case of deploying IoT in Montréal. Figure A is a flowchart of this system's technological and analytical components.

[3] We have adopted a pluralist approach to ethics in this project aimed at identifying issues raised in the literature, whatever the authors' ethical viewpoint. This approach, which has also been used elsewhere (such as the EU's ETICA project), permits taking different outlooks and interpretations into account and delineating coexisting perspectives in this field (Stahl, 2011).

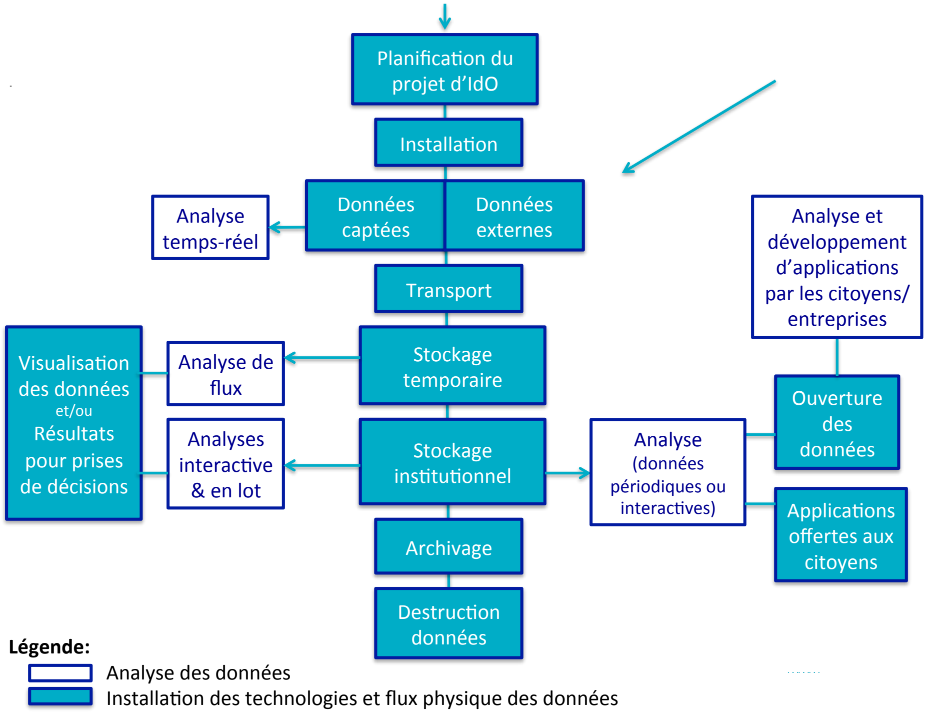

Planification du projet d'IdO
Installation
Analyse temps-réel
Données captées
Données externes
Analyse et développement d'applications par les citoyens/ entreprises
Transport
Visualisation des données et/ou Résultats pour prises de décisions
Analyse de flux
Stockage temporaire
Ouverture des données
Analyses interactive & en lot
Stockage institutionnel
Analyse (données périodiques ou interactives)
Applications offertes aux citoyens
Archivage
Destruction données
Légende:
Analyse des données
Installation des technologies et flux physique des données

Figure A: IoT Technological and Analytical Flowchart

Step one involves planning the urban IoT installation/implementation project. Next, sensors, as well as hardware and software for operating them, will be deployed. Data will then be collected from these sensors, as well as from external databases, such as social media, and transferred to storage, and eventually archival, sites. Data will be processed (aggregation, possible anonymization, etc.) at different sites. While these intermediate steps do not appear on the flowchart, they are important. Data analysis (including predictive and prescriptive) is then analyzed at different points. These analyses primarily serve two key audiences—municipal decision makers and their partners (such as the STM), and the public, including residents and businesses, by releasing open data and developing apps for Montrealers designed to improve the quality of urban life. Section 3.2.1 of this report describes this system's technical details. It also explains why such a system must evolve in the presence of big data and not in a vacuum. Once collected and released, data is combined with existing data taken from inside and outside the city administration.

This system breaks down into four main phases in terms of the ethical issues identified in our review of the literature:

1. Infrastructure planning and maintenance.
2. Data collection and storage (including processing).
3. Internal/external data analysis.
4. Release of open data and establishment of public, digital services.

Social Acceptability

We cannot confidently identify issues pertaining to the social acceptability of IoT in the smart city, since the existing literature contains so few studies on this topic. However, Section 10 of this report lists existing studies focusing on social acceptability during the use phase, particularly in terms of the value and utility of products, services and infrastructure.

We cannot present a clearly defined list of social acceptability issues, since there are so few studies on the topic. This report accordingly presents ethical issues and concerns identified in the literature that could be sources of public resistance to the urban IoT project and mar its social acceptability. These ethical issues and concerns appear in the following figure, which serves as an executive summary of our literature review's results.

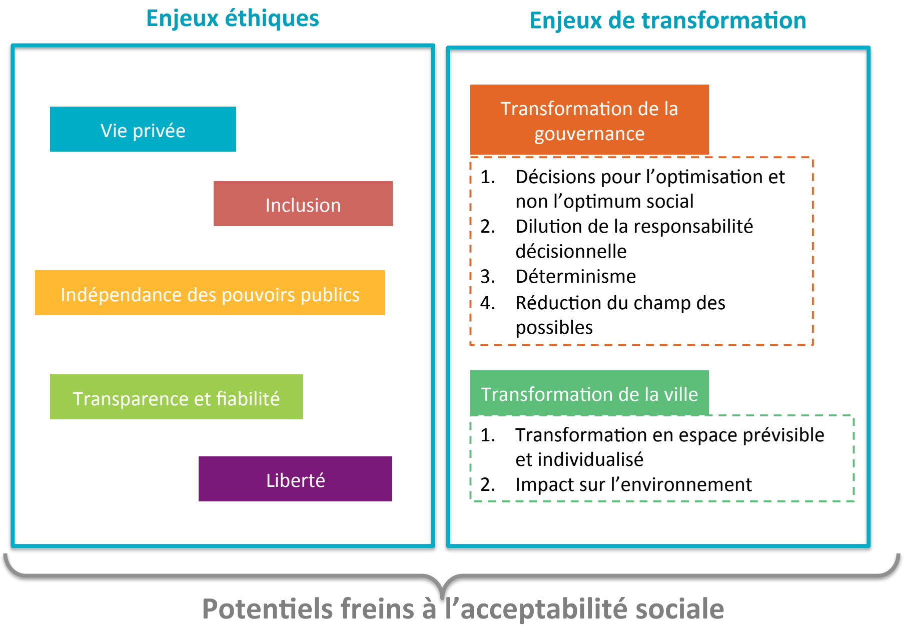

Enjeux éthiques
Vie privée
Inclusion
Indépendance des pouvoirs publics
Transparence et fiabilité
Liberté
Enjeux de transformation
Transformation de la gouvernance
1. Décisions pour l'optimisation et non l'optimum social
2. Dilution de la responsabilité décisionnelle
3. Déterminisme
4. Réduction du champ des possibles
Transformation de la ville
1. Transformation en espace prévisible et individualisé
2. Impact sur l'environnement
Potentiels freins à l'acceptabilité sociale

Figure B: Potential Obstacles to Social Acceptability

Our review of the literature revealed six ethical issues, falling under five headings—privacy, social inclusion, separation of government and business spheres, transparency, reliability and freedom.[4] These categories are based on the various subjects mentioned in the literature, as well as existing classifications.[5]

Our study also highlighted seven concerns, falling under two main headings: those pertaining to changes in municipal governance and those to transformation of the city itself. These concerns do not qualify as ethical issues, since they are not clearly associated with basic values or principles. Yet they are identified concerns that could affect a project's social acceptability.

We have focused on factors of change in modes of governance inherent to IoT. These factors, which have major implications for the city administration and residents, are discussed in Section 9. For these reasons, they are key elements to be considered in any discussion on the social acceptability of the IoT project.

Ethical Issues

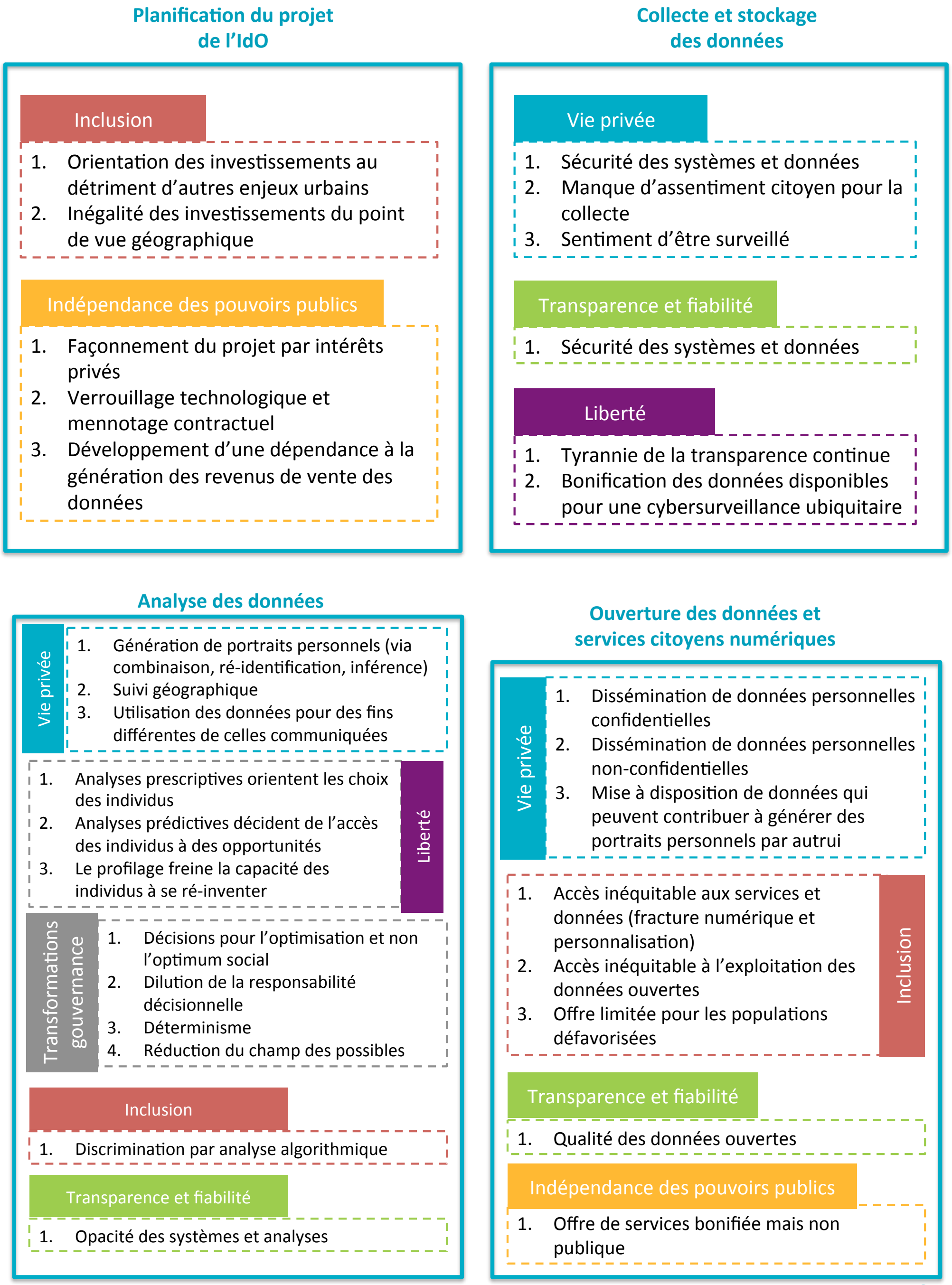
Sections 4 to 8 cover each of the six identified ethical issues, grouped by the kinds of threats the IoT project poses to these fundamental values and principles. We more closely examine situations and activities specific to IoT that give rise to such issues. These threats are also grouped by IoT phase. For example, threats to privacy in data collection (such as lack of public consent to such collection) are different from those arising from the release of open data (possible dissemination of confidential information).

Figure C, below, outlines the ethical issues described in the report, with respect to the four main phases of IoT system: data analysis, release of open data, and public, digital services. These boxes present the ethical issues corresponding with each phase and the specific threats that cause these issues. This report explains all of these factors in depth.

Because of the importance of possible changes in the governance system and their coverage in this report, they are identified alongside ethical issues in the following figure.

[4] Transparency and reliability are considered together, in the same section of the report, since they share numerous characteristics.

[5] Such as those mentioned in a report for the European Parliament's LIBE Committee (European Parliament, 2015), the ETICA Project (Stahl, 2011) and the EU's Ethics Subgroup IoT (van den Hoven, 2016).



Planification du projet de l'IdO

Inclusion

1. Orientation des investissements au détriment d'autres enjeux urbains
2. Inégalité des investissements du point de vue géographique

Indépendance des pouvoirs publics

1. Façonnement du projet par intérêts privés
2. Verrouillage technologique et mennotage contractuel
3. Développement d'une dépendance à la génération des revenus de vente des données

Collecte et stockage des données

Vie privée

1. Sécurité des systèmes et données
2. Manque d'assentiment citoyen pour la collecte
3. Sentiment d'être surveillé

Transparence et fiabilité

1. Sécurité des systèmes et données

Liberté

1. Tyrannie de la transparence continue
2. Bonification des données disponibles pour une cybersurveillance ubiquitaire

Analyse des données

Vie privée

1. Génération de portraits personnels (via combinaison, ré-identification, inférence)
2. Suivi géographique
3. Utilisation des données pour des fins différentes de celles communiquées

Liberté

1. Analyses prescriptives orientent les choix des individus
2. Analyses prédictives décident de l'accès des individus à des opportunités
3. Le profilage freine la capacité des individus à se ré-inventer

Transformations gouvernance

1. Décisions pour l'optimisation et non l'optimum social
2. Dilution de la responsabilité décisionnelle
3. Déterminisme
4. Réduction du champ des possibles

Inclusion

1. Discrimination par analyse algorithmique

Transparence et fiabilité

1. Opacité des systèmes et analyses

Ouverture des données et services citoyens numériques

Vie privée

1. Dissémination de données personnelles confidentielles
2. Dissémination de données personnelles non-confidentielles
3. Mise à disposition de données qui peuvent contribuer à générer des portraits personnels par autrui

Inclusion

1. Accès inéquitable aux services et données (fracture numérique et personnalisation)
2. Accès inéquitable à l'exploitation des données ouvertes
3. Offre limitée pour les populations défavorisées

Transparence et fiabilité

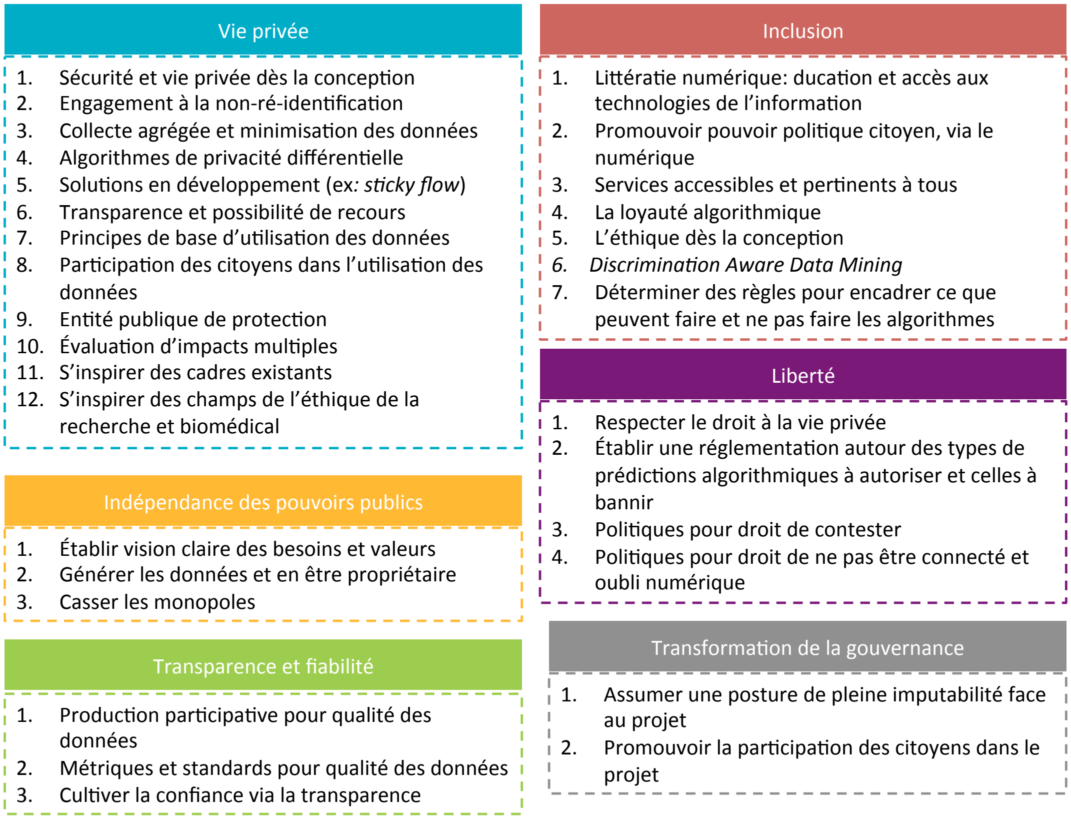
1. Qualité des données ouvertes

Indépendance des pouvoirs publics

1. Offre de services bonifiée mais non publique

Figure C: Summary of Identified Issues and Related Threats

For each issue covered, the report also describes solutions identified in the literature (presented in Figure D).



Vie privée

1. Sécurité et vie privée dès la conception
2. Engagement à la non-ré-identification
3. Collecte agrégée et minimisation des données
4. Algorithmes de privacité différentielle
5. Solutions en développement (ex*: sticky flow*)
6. Transparence et possibilité de recours
7. Principes de base d'utilisation des données
8. Participation des citoyens dans l'utilisation des données
9. Entité publique de protection
10. Évaluation d'impacts multiples
11. S'inspirer des cadres existants
12. S'inspirer des champs de l'éthique de la recherche et biomédical

Indépendance des pouvoirs publics

1. Établir vision claire des besoins et valeurs
2. Générer les données et en être propriétaire
3. Casser les monopoles

Transparence et fiabilité

1. Production participative pour qualité des données
2. Métriques et standards pour qualité des données
3. Cultiver la confiance via la transparence

Inclusion

1. Littératie numérique: ducation et accès aux technologies de l'information
2. Promouvoir pouvoir politique citoyen, via le numérique
3. Services accessibles et pertinents à tous
4. La loyauté algorithmique
5. L'éthique dès la conception
6. *Discrimination Aware Data Mining*
7. Déterminer des règles pour encadrer ce que peuvent faire et ne pas faire les algorithmes

Liberté

1. Respecter le droit à la vie privée
2. Établir une réglementation autour des types de prédictions algorithmiques à autoriser et celles à bannir
3. Politiques pour droit de contester
4. Politiques pour droit de ne pas être connecté et oubli numérique

Transformation de la gouvernance

1. Assumer une posture de pleine imputabilité face au projet
2. Promouvoir la participation des citoyens dans le projet

Figure D: Summary of Solutions Identified

These proposed solutions are discussed in succession in Sections 4 to 9, without discussing the thoughts or opinions of the reports' authors as to their merit, maturity or compatibility. However, these solutions share some points:

- Transparency.
- Potential remedies.
- Public participation.
- Determination of the project's basic principles.

Transparency is identified in different works as a potential solution applicable to all data phases—collection, use, release and (possible) sale, as well as to decisions made from the data use and any breaches—and appears several times as a potential solution. Naturally, it would be difficult or impossible to discuss all these topics in detail. However, the idea of transparency on key principles, guidelines and intentions, constantly recurs in several of the proposed solutions.

Giving the public access to a **grievance redress mechanism** with respect to privacy, algorithmic bias and cybersurveillance has been suggested more than once. While this mechanism would give people the right to ask questions and file complaints, it would also create a climate in which government officials must maintain audit trails of their decisions and procedures.

Public participation in the urban IoT project is a dominant theme. It is discussed in Section 4 (Ethical Issue: Privacy), when the authors recommend transparency in data collection and use, as well as in suggestions by some figures that the public participate in the actual use of the data, through information and apps placed at their disposal, giving free reign to creativity and innovation. Similarly, social inclusion is seen as a key factor in ethical issues pertaining to social inclusion itself, and to changing governance systems. Participation is considered important in all IoT phases—planning, data collection and storage, data analysis, and open data and services.

Finally, another concept intrinsic to several of the solutions mentioned is the need to define the **project's basic values and requirements** clearly. Doing so is crucial for several reasons. The section on privacy describes this need in terms of defining principles and values that can guide data collection and use to minimize privacy infringements. Delineating these principles is also important during interactions with the privacy sector in planning and implementing IoT technology, where vendor goals may differ from those of the city administration, or the common good.

Privacy

We weighted our consideration of the different ethical issues in terms of their prominence in the literature, rather than equally. The issue of privacy accordingly dominates this report because of its importance and the threat IoT poses to it, as well as its presence within the complex existing legal framework.

Section 4.2, on IoT's legal framework, starts with a review of the principles that have guided data collection and use over the past five decades. Section 4.3 then describes the crisis in personal data protection due to various aspects of Economy 4.0, such as the installation of sensors in public areas, access to vast quantities of data and algorithm analysis (Rubinstein, 2013; Crawford and Schultz, 2014; Narayanan, et al., 2016; Mantelero, 2014; Tene and Polonetsky, 2013; Gaughan, 2016). In the particular case of urban IoT deployment, the following issues are of particular note:

- Difficulty of giving notice and obtaining consent for sensor-based data collection.
- Difficulty of ensuring[6] that personal data is anonymized, in a context of big data and predictive analytics.
- Surge in creation of "personal" data.
- Difficulty of promoting the proportionality principle or minimal data collection in a big data environment.

In other words, there is a clear regulatory gap with respect to ensuring the privacy of IoT data.

Social Inclusion

Ethical issues pertaining to social inclusion also play a key role in the report. This section explores the digital divide and its impact on people's abilities to use smart city services, as well as to engage with the released data and play a key role in using it.

The section also considers the discriminatory potential of algorithm analysis, which profiles groups for various reasons. Algorithms classify and simplify information according to their programmed values. They are designed to accentuate similarities between members of a particular group, as well as differences between preconceived categories. This means algorithms are inevitably "embedded with values" defined by developers' operating parameters, as configured by users (Mittelstadt, 2016). The literature is replete with examples of such algorithms causing discrimination.

The section also discusses recommendation algorithms, which refer consumers to new markets by suggesting products, people, services and organizations. Doing so makes it easier to find "similar" information, but can result in unequal access to various opportunities for different individuals.

Finally, the report also looks at other issues (separation of the government and business spheres, transparency/reliability, and freedom), although somewhat more succinctly, given their limited coverage in the literature.

[6] Anonymization eliminates the link between the data and a specific individual (Richards and King, 2004).

Changing Modes of Governance

The literature on social issues associated with smart cities and IoT does not suggest that IoT will result in basic changes in governance.

While these issues cannot be qualified as "ethical," they remain important in terms of their impact on day-to-day administration of the city and its dealings with residents.

Our literature review identifies the factors inherent to this transformation. All relate to the technological bias of IoT-based governance, where technology plays a prevailing role in governance and decision-making. This technological bias engenders a depoliticization of issues the smart city is expected to address. In other words, we present this immense urban project primarily as a technological, apolitical and common sense initiative, minimizing debate on proposed political solutions and priorities, and thereby reducing the potential for social opposition (Douay and Henriot, 2016).

All of the main factors involved in the transformation of municipal governance are present in the data analysis phase. They are:

- Decisions aimed at optimization, rather than the social optimum or root causes.
- Integration resulting in a reduction or loss of decision-making responsibility.
- Deterministic worldviews.
- Diminished range of analytical scenarios.

Conclusion

The literature review groups ethical issues and concerns about urban IoT that could damage the IoT project's social acceptability.

Our discussion gives equal emphasis to the various issues and solutions. We do not wish at this stage of our work to weigh arguments, solutions or ideas. While we believe this process is essential, it will be conducted at a later phase, in close conjunction with the city, to ensure the impartiality that is expected in a review of this kind.

Contents

Tables

Figures

Abbreviations and Acronyms

SA	Social acceptability
BAPE	Bureau d'audiences publiques pour the environment
BD	Big data
CESE	Conseil économique, social et environmental (France)
CEST	Commission à l'éthique en sciences et technologies du Québec
CIRAIG	Centre international de reference sur le cycle de vie des products, procédés et services
DADM	Discrimination Aware Data Mining
DPA	Differential Privacy Algorithm
IDF	Israel Defense Forces
FTC	Federal Trade Commission
AI	Artificial intelligence
ICF	Intelligent Community Forum
IoT	Internet of Things
ICT	Information and communication technologies
PSTRE	Problem solving in technology-rich environments
RFID	Radio frequency identification
SPVM	Service de Police de la Ville de Montréal
STM	Société des Transports de Montréal
IT	Information technologies
VGI	Voluntary geographical information

1 Introduction

1.1 The Project

Since 2014, Montréal has been implementing a strategic initiative to become an internationally renowned leader among smart and digital cities. Montréal plans to develop on its own—and in partnership with residents—technological solutions to the metropolis's key challenges, which it will deploy transparently, with advanced technologies and on a human scale. The city's fourfold strategy is to collect/release data to achieve better value for money and promote public participation and innovation, communicate information and foster public connectivity, coordinate digital/smart services for the public, and work with different parties to create networks for and accelerators of innovation (Ville de Montréal, 2017).

Installation of technological infrastructure, and in particular, the development of an Internet of Things in the city, is central to this strategy, which will culminate in the construction of technological and analytical systems for data collection, storage and analysis. IoT also means implanting a multitude of sensors throughout the city to collect a vast variety of data on the metropolis's assets and activities. A key feature of the digital strategy is the collection of data from sensors and other sources for internal use by the city and its partners, accompanied by external use through big data releases. The city initially plans to focus the use of such data on Montréal's urban priorities, like intelligent traffic management, the environment, urban asset management (furniture, vehicles) and public safety.

While the use of collected data presents opportunities for innovation and for improving Montreal's quality of life, it raises ethical issues and risks that could engender social opposition. In particular, the mere use of IoT's technical and analytic framework, along with the many changes that will result from new forms of interaction between residents and their municipal administration, constitute issues that must be identified and resolved.

This report seeks to support the city in its consideration of this topic by outlining potential issues of ethics and social acceptability involved in using IoT in the city and finding solutions. In broader terms, it was produced under Batch 5 of the Internet of Things Standards Formulation Project and will serve as a stepping-stone to subsequent project phases:

- Defining a conceptual framework for developing a program to analyze, manage and address issues of ethics and social acceptability associated with the IoT project.
- Establishing the basis of a proposal for establishing a city hall advisory committee to deal with the ethical, legal and social ramifications of urban IoT deployment.
- Identifying topics and issues in this field to be considered in greater depth.

1.2 Document Structure

This report has 12 sections.

Section 1 is the introduction.

Section 2 is a preface on questions concerning Montréal's IoT project in the context of ongoing debates on the greatest revolution in urban architecture in modern history and its impact on people. The preface describes the IoT project as the tangible expression of a rebooted urban structure organized around the convergence arising out of Economy 4.0.

Section 3 describes the methodology applied to our literature review and delineates the scope of the IoT system considered by the project.

Sections 4 to 9 each cover urban IoT issues named in the literature, as well as the change in governance mechanisms. Ethical issues pertain to privacy, social inclusion, separation of the government and business spheres, transparency and reliability/freedom. Each issue is examined in terms of threats the IoT project poses to our fundamental social values and principles. We also outline potential solutions identified in the literature for dealing with these issues.

Section 10 defines social acceptability and describes how the literature has treated the connected city's issues of social acceptability through the present, as well as potential solutions.

Section 11 is the conclusion.

2 PREFACE: Urban Architecture's Human Impact

2.1 Evolution of Urban Infrastructure: Classic Social Science

Urban evolution has long been a classic social science topic. The city is an ideal laboratory for researchers studying the emergence of new social dynamics, and for those interested in social inertia (Fijalkow, 2007).

Even in his day, Georg Simmel (1858-1918) focused on how the city dweller's "mental life" is shaped by urban dynamics. In his notable 1903 essay, *The Metropolis and Mental Life,* Simmel sought to explain the dramatic changes in personal behaviour due to the emergence of vast metropolises. At the turn of the 19th century, Simmel lived in Berlin, which was undergoing relentless, fast-paced change under the pressure of strong demographic growth.

Simmel's *vertical habitat*—the metropolis—is the force driving reconfiguration of the social rules of a small town (where everyone knows everyone else), and thus alters personal bonds. Simmel evaluated the new dynamics of social interaction through *The Stranger's* perspective.[7] Based on this work, he ultimately defined a philosophy of urban sociology.

Urban architecture is not, accordingly, merely the reflection of a social situation, but an engine of social change. We plan to develop this important hypothesis in our discussion on implementing urban IoT.

Nathaniel Robert Walker[8] recently published an excellent article criticizing his colleagues for underestimating industry's role in changing urban lifestyles (Walter 2016), and, in particular, the importance of carmakers in defining land use planning.

The example considered by Walker is of particular interest to us, because his study of marketing campaigns for new urban designs in the mid-20th century revealed that General Motors was a key player in this effort. Walker's research demonstrates that one of GM's goals was to make all Americans dependent on cars by restructuring urban infrastructure (housing, roads, public transit and services), as we see in in Edward Bunker's *No Beast So Fierce* (2016), heralding the emergence of Los Angeles' car culture of the 1970s.

[7] In Simmel's view, city life produces two mutually supporting dynamics: (1) individualism and (2) modern times. It describes the urban fabric as a form of social consciousness and the city as a way of life. The work of Belgian sociologist Jean Remy updated Simmel's approach to contemporary cities by underscoring the importance of proximity and distance in our dealings with others (Germain, 1997).

[8] Assistant Professor of Architectural History.

Why begin this introduction with these references to Georg Simmel and General Motors?

Both, we believe, provide excellent contexts for studying the connected urban infrastructure typical of IoT. As Georg Simmel and then Max Weber (1864-1920) in his book *The City*,[9] suggested, urban infrastructure implies specific behaviour patterns and it is therefore appropriate to consider the social impact (social and ethical acceptability) of digital urban infrastructure.

Furthermore, as Walker mentioned, we must identify the industrial purview of the smart city. Is the smart city simply an industrial project? Simmel wrote that the vertical habitat is the contemporary cocoon. In light of this clear insight, we shall revise urban connectivity in its guise of a modern cocoon, presiding over deployment of the convergence propelling Economy 4.0.

> *A Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.* (Schwab, 2016: 1).

2.2 Using Technological Innovation to Resolve Urban Challenges

2.2.1 More Than Half the World's Population Lives in Cities

The world became a predominantly urban society in 2007 when, according to estimates, cities became responsible for three quarters of all economic activity (Brender, 2012). As we know, cities only occupy 2% of the globe's surface and now house 50% of the planet's population—a figure that, according to forecasts,[10] will leap to 60% in 2030 and 70% in 2050. Cities consume 75% of all energy produced and are the source of 80% of all CO_2 emissions. All sectors associated with urbanization (transportation, building construction/maintenance, housing, waste management and energy) share trends responsible for sustainability problems. Many sociologists believe such problems are breeding grounds for economic disparities and social exclusion (William Wilson, 1987; Desmond, 2012; Goffman, 2009). Furthermore, the increased demographic weight of major urban centres gives them greater political and economic clout (Doran, 2014). Cities are increasingly behaving like autonomous international stakeholders (Olive, 2015; Le Gales, 1995), seeking to build on their reputations as innovative hubs among experts, the media and the public.

[9] As noted by Damien Augias, in *"Max Weber et Georg Simmel nous parlent des villes," Le Monde*, 28.04.2014.

[10] The 2016 The United Nations Conference on Housing and Sustainable Urban Development (Habitat III), in Quito, adopted a *New Urban Agenda* to make cities more inclusive, secure, resilient and sustainable. The smart city was the subject of a working paper (May 31, 2005) defining the role and status of digital urban infrastructure needed to address societal challenges. http://habitat3.org/wp-content/uploads/21-Habitat-III-Issue-Paper-21_Villes-intelligentes.pdf

2.2.2 City Life Transformed by Technological Innovation

There are now over 7 billion cell phone accounts in the world, compared to just 738 million in 2000. Around the world, 3.2 billion people are Internet users, with 2 billion of them in developing nations. Mobile broadband was available across 47% of globe in 2015, 12 times more than in 2007. In 2015, 69% of the planet's population had 4G access, up from 45% in 2011 for 3G mobile technology. Most aspects of the new urban agenda draw on the roles and abilities of information and communication technologies to meet goals and overcome hurdles (please refer to the *Habitat III Policy Papers*), offering the international community new opportunities for and innovative means of making cities secure, resilient and sustainable spaces for everyone.

2.2.3 Origin and Dissemination of the Smart City Concept

The first urban digital infrastructure deployment dates from the early 2000s. Launched by the South Korean government in 2003, the smart city of Songdo was completed in 2015.[11]

However, former US President Bill Clinton has been credited with promoting the term *Smart City*. Clinton apparently recognized the convergence of two millennial revolutions: (1) massive urbanization and (ii) proliferation of information technologies. Clinton believed that technological innovation would help regulate city living:

> *The idea seemed to be the outgrowth of a challenge proposed in 2005 by the former US president to John Chambers, president of Cisco, manufacturer of digital network equipment: why not use these amazing resources to make cities more sustainable? . . . At the 2005 Second World Summit of Cities and Local Authorities on the Information Society in Bilbao, participants 'defined a common strategy' for giving information and communications technologies access to their territories. This was the first time that such a meeting, organized by the UN and traditionally reserved for states, was open to local officials, private businesses and civil society . . . Cisco will study the topic (on a $25 M budget) and market the results in 2010. In 2008, IBM got onboard this first wave of investment (smart cities will be ICT's biggest customers over coming years), with its Smarter Cities initiative"* (Pisani, 2015).

[11] http://songdoibd.com/

2.3 Oscillating Between Utopia and Dystopia[12]

Urban infrastructure is altered by installing multitudes of sensors. Integration of these hi-tech systems into the urban habitat transforms it into a digital infrastructure (Rolland-Villemot, 2015). The data collected from digital sensors is a new commodity, with the potential to optimize the mobility and security of urban infrastructure, minimize contamination, and create new issues, while amplifying old challenges.

Based on classical sociological theory (Simmel, Weber and Marx), it is highly likely that Economy 4.0 will inexorably change contemporary urban life in posing new issues of ethics and social acceptability. Our task is to conduct a sociotechnical study—but the reader will quickly realize that our focus has expanded to embrace urban policy, as well as deliberative governance, public participation, protection of privacy and the "information commons."

Readers of this report will also note the emphasis we have placed on adopting new deliberative mechanisms for this groundbreaking IoT technology. A vast number of ideas and potential solutions have been proposed to help decision-makers deal with Innumerable with often-thorny problems.

While some of these solutions will turn out to be "right," other approaches might ultimately prove more productive. Only time will tell. Faced with the highly interconnected challenges of the Anthropocene Era, and, being wrong more often than we think, Mistakes, with a capital M, are not only sure to occur but will be welcome if and only if multi-party assessment and discussion mechanisms are present and functional. Otherwise, the IoT utopia could quickly turn into an Orwellian nightmare.

[12] Dystopic literature depicts an imaginary society built around human fears https://mondedulivre.hypotheses.org/337

3 Scope and Technique of the Literature Review

3.1 Technique

We based the methodology of our literature review on two core issues:

1. *What ethical issues are associated with IoT in a smart city?*
2. *What issues of social acceptability pertain to IoT in a smart city?*

We should start by defining what we mean by the Internet of Things in Montréal. We did so by consulting the literature, as well as conducting interviews with Montréal city representatives. We also explored our study's two fundamental concepts—*ethical issues* and *social acceptability issues*—to determine their scope within this report. Finally, we conducted research focusing on these questions.

Our literature search on issues of ethics and social acceptability focused on scientific texts (books and journals), but included such grey literature as reports from governments (primarily from the US and Europe) and international organizations, as well as blogs by recognized researchers, journalists and commentators. The literature covered a range of disciplines, including the social sciences, computer science, geography, law and ethics, as well as such subfields as urban studies, critical data studies, new technology ethics, cyberethics, IT ethics and IoT ethics.

We applied two approaches, often hand-in-hand, to our review of the literature. The first involved keyword searches (*smart city*, *Internet of Things*, *ethical issues* and *social acceptability*) relating to the study, in different permutations.[13] Then we included keywords found in our readings that pertain more specifically to issues of ethics and social acceptability. We also added such keywords as *big data* and *algorithm analysis,* which relate to IoT's fundamental technological and analytical concepts.

One challenge of the literature review was that many relevant sources often did not pertain directly to the smart city. Various texts on the ethical issues of IoT considered big data and algorithm analysis, but not in terms of the smart city. In particular, a number of sources discussed IoT in terms of current personal uses (smartphones and FitBit watches), rather than sensors installed by city government. The team producing this report applied common sense in extrapolating some of this information to the smart city context.

[13] We searched the scientific literature with Virtuose, Scopus and Google Scholar. Google Scholar was used for grey literature. Our second research strategy involved identifying references in the bibliographies of texts consulted.

3.2 The IoT System Discussed in the Literature Review

The literature review covered topics specific to IoT's deployment in Montréal. The technological and analytical framework of the planned system appears below, in Figure 1.

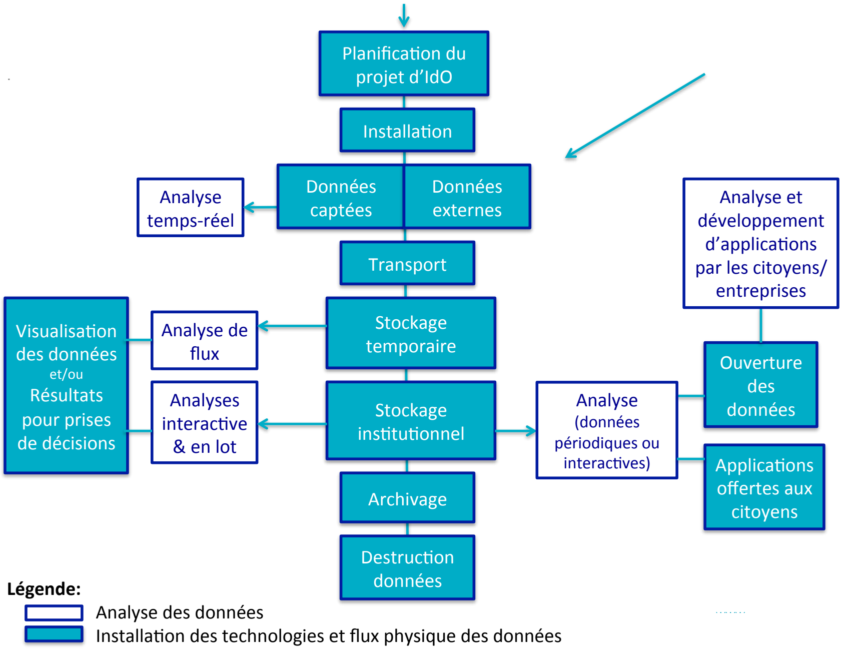

Planification du projet d'IdO
Installation
Données captées
Données externes
Analyse temps-réel
Transport
Analyse et développement d'applications par les citoyens/ entreprises
Visualisation des données et/ou Résultats pour prises de décisions
Analyse de flux
Stockage temporaire
Ouverture des données
Analyses interactive & en lot
Stockage institutionnel
Analyse (données périodiques ou interactives)
Applications offertes aux citoyens
Archivage
Destruction données
Légende:
□ Analyse des données
■ Installation des technologies et flux physique des données

Figure 1: IoT's Technological and Analytical Framework

Step one is planning the urban IoT installation/implementation project. Next, sensors, as well as hardware and software for operating them, will be deployed. Data will then be collected from these sensors, as well as from external databases, such as social media, and transferred to storage, and eventually archival, sites. Data will be processed (aggregation, possible anonymization, etc.) at different sites. While these intermediate steps do not appear on the flowchart, they are important. Data analysis (including predictive and prescriptive) is then performed at different points. These analyses primarily serve two key audiences—municipal decision makers and their partners (such as the STM), and the public, such as residents and businesses, by releasing open data and developing apps for the public, designed to improve the quality of urban life.

This system evolves in the presence of big data and not in a vacuum. Newly collected data will—following its release or the development of apps for the public—be combined with existing bases, from inside and outside the city, a central feature of the city's digital strategy.

For the sake of simplicity, this system can be broken down into four main phases highlighting the ethical issues identified in our literature review:

- Infrastructure planning and maintenance.
- Data collection and storage (including processing).
- Internal/external data analysis.
- Releasing open data and developing apps for the public.

Each of these four steps corresponds with one or more of the multiple phases involved in creating IoT's technical and analytical framework, as shown below in Figure 2. Data processing (but not analysis), for example falls, for the moment, under "data collection and storage."

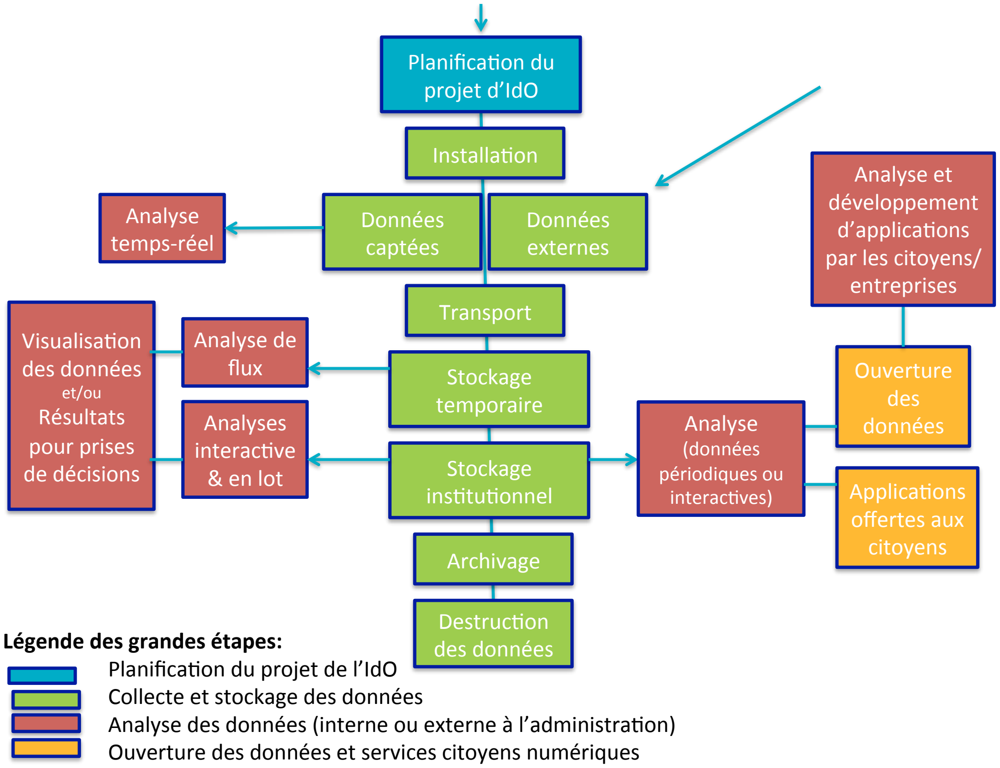

Planification du projet d'IdO
Installation
Données captées
Données externes
Analyse temps-réel
Analyse et développement d'applications par les citoyens/ entreprises
Transport
Visualisation des données et/ou Résultats pour prises de décisions
Analyse de flux
Stockage temporaire
Ouverture des données
Analyses interactive & en lot
Stockage institutionnel
Analyse (données périodiques ou interactives)
Applications offertes aux citoyens
Archivage
Destruction des données
Légende des grandes étapes:
Planification du projet de l'IdO
Collecte et stockage des données
Analyse des données (interne ou externe à l'administration)
Ouverture des données et services citoyens numériques

Figure 2: Simplified System in Question

3.2.1 Highlighting Various Components

This system's technical and analytical elements include:

- Technologies that generate and collect data, while transporting it to municipal servers (cams, sensors, RFID tags, Wi-Fi, etc.).
- Data from municipal sensors and external sources, such as social media and other sites where people communicate directly (or not) with the city.
- Internal/cloud storage and archival sites.
- Analytical tools that convert data to information, including all predictive and prescriptive data analysis techniques involving statistical, algorithmic and machine-learning models.
- Organizational structures that support collaboration and innovation and improve municipal services with new sources of information, such as open data, permitting consultation of data or entire databases.[14]

It should be noted that IoT is not evolving in isolation, but draws on amalgamations of data, drawn from a variety of sources, to support analyses by municipal government, as well as residents and business with access to such open data. According to Mohnanty, et al. (2016), a smart city is based just as much on the use of sensors as on big data.

3.3 Ethical/Social Acceptability Issues and Solutions: Definitions and Method

3.3.1 Ethical Issues: Definitions and Method

As we know, ethics is a statement of the core values and principles that should guide and direct our interactions with others. These values and principles give meaning to our lives and enable us to distinguish, in a given context, between good/evil, right/wrong, and appropriate/inappropriate. In other words, an ethical issue arises whenever a moral principle or a value comes into play in a situation (Commission de l'éthique en science et technologie du Québec, 2017).

There are several ethical traditions. Most of the literature we studied amply covers issues arising from IoT, along with its intrinsic and related technologies, under the very broad heading of *applied ethics*, a subfield focusing on tangible situations (Commission de l'éthique en science et technologie du Québec, 2017), to which numerous approaches, as well as recommended/discussed frameworks apply.

[14] Adapted from *National League of Cities*, which identified three core components of the smart city. http://www.nlc.org/article/new-report-on-smart-cities-released-by-national-league-of-cities

In this project, we have adopted a pluralist approach aimed at identifying issues raised in the literature, whatever the different authors' perspectives. This approach, which is used elsewhere as well (as in Europe's ETICA Project[15]), sheds light on a variety of viewpoints and interpretations, while highlighting co-existing outlooks in the field (Stahl, 2011).

As part of this approach, we listed the various issues that were raised. Next, we grouped the issues in logical categories corresponding to the fundamental values that might be eroded or undermined by deployment of urban IoT. The categories are privacy, social inclusion, freedom, transparency/reliability, and separation of the government and business spheres. These groupings naturally drew on those appearing in the literature, and in particular, those mentioned in a report for the EU's LiBE Committee (European Parliament, 2015), the ETICA Project (Stahl, 2011) and the writings of Jeroen van den Hoven (2016).

We weighted our consideration of the different ethical issues in terms of their prominence in the literature, rather than equally. The issue of privacy accordingly dominates this report because of its importance (van den Hoven, 2016) and the fact that these issues are interwoven with numerous legal issues and frameworks.

3.3.2 Social Acceptability: Definitions and Method

Social acceptability is a controversial term, with much debate over its definition (Gendron, 2014; Battelier, 2015). The expression generally refers to the idea that a group or the parties concerned (such as the public), consent to a project that has been offered to them. Appendix G gives an overview of different definitions for the expression. For this project, we have applied that of Corinne Gendron (2014), which seems to represent a certain consensus and includes a number of concepts based on other definitions. Gendron (2014) defines social acceptability as "the public endorsement of a plan or decision based on the collective judgement that the project or decision is better than the known alternatives, including the status quo."

In line with this definition, our review of the literature focused on documents discussing public consent for urban IoT projects and their inherent or IoT-related core technologies. As mentioned in Section 10, the few studies on this topic do not at this point serve to identify "issues of social acceptability" for the smart city. We can, however, list ethical issues and concerns that might give rise to public resistance toward an urban IoT project and thus constitute an impediment to the project's social acceptability.

[15] Project on ethical issues of emerging technologies, funded by the European Union.

3.3.3 Approach to Solutions

The potential solutions identified in this report are “possibilities” rather than actual “solutions” and describe strategies for dealing with identified issues. They may represent solutions already in application, those under development and those merely at the idea stage. They reflect our findings in the literature, not the authors’ opinions. They were selected if they met at least one of the following criteria, although many met both:

1. Multiple writers have identified the potential solution.
2. It is sufficiently formulated to permit its explanation.

The potential solutions cited in the report do not include all those listed in the literature. Additional time and resources would be required to clarify their status properly.

Box 1: Improved Classifications of Potential Solutions

In this report, potential solutions to each ethical issue are presented following our discussion of the issue and are grouped by “ethical concern.” However, it would subsequently be useful to group them by the organization and writer proposing each option. It would be especially useful to map these solutions by government (such as the European Union and United States). Potential solutions appearing in the literature that are not well developed, but are sensible, relevant and generic, could be presented in a future study.

4 Ethical Issue: Privacy

In 2014, the United Nations High Commissioner for Human Rights (UNHCR, 2014) published a warning on the threats to privacy of data collection, preservation and incidental use (UNHCR, 2014). Many national governments and supranational bodies have set up special committees on this very topic over the past few years, notably within the European Union and the United States.

4.1 What is Privacy?

There has been much debate about how privacy is defined. It can be seen as personal freedom from any physical intrusion into or interference with a person's life (for example, in terms of his or her choices, plans and decisions), as well as a person's ability to control access to and use of his or her personal information (Tavani, 2004).

Many people maintain that privacy is a function of the context in which information is exchanged, rather than the nature of the communication (Nissenbaum, 2004; Barocas and Nissenbaum, 2014;[16] Gaughan, 2016). According to this viewpoint, specific "information rules" apply to each exchange, which is why people may or may not want to protect their privacy in a public space, such as a city.

4.2 Evolution of the Legal Framework

Any discussion of privacy must consider its legal framework, which governs personal data protection. This section provides a brief overview of the topic, while Appendix B explores it in detail.

North American privacy protection legislation is largely based on the *Fair Information Practice Principles* (FIPPs) established in the United States in the 1970s. These principles then evolved with the creation of various national and international policies, such as the *OECD Guidelines on the Protection of Privacy and Transborder Data Flows*, the Federal Trade Commission's (FTC's) *Privacy Shield Principles* and the *European Commission Directive on Data Protection* (Richards and King, 2004; Cate, 2006).[17]

[16] Nissenbaum (2004, 2014) has endorsed Helen Nissenbaum's theory of contextual integrity (2004, 2014), which Appendix 1: Privacy explains in detail.

[17] Recently updated as the *General Data Protection Regulation* (GDPR), implemented in May 2018 (European Parliament, 2016).

This set of guidelines incorporates the concepts mentioned in Figure 3, above.

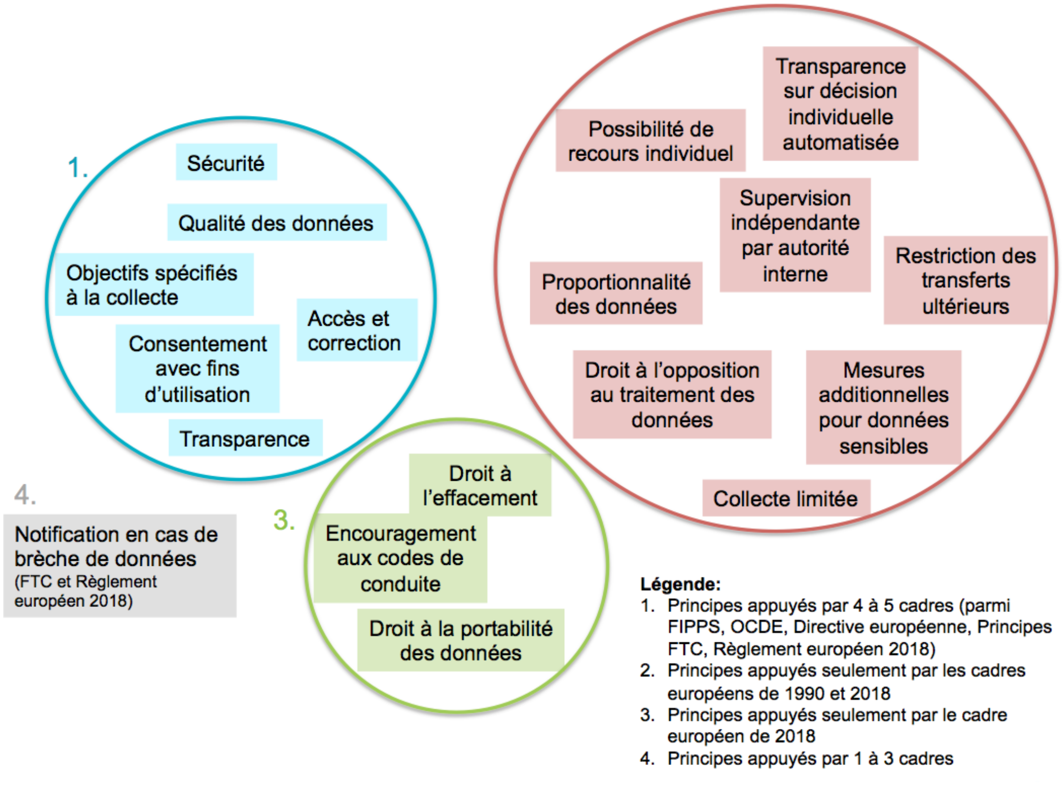

1.
Sécurité
Qualité des données
Objectifs spécifiés à la collecte
Accès et correction
Consentement avec fins d'utilisation
Transparence
Transparence sur décision individuelle automatisée
Possibilité de recours individuel
Supervision indépendante par autorité interne
Proportionnalité des données
Restriction des transferts ultérieurs
Droit à l'opposition au traitement des données
Mesures additionnelles pour données sensibles
Collecte limitée
4.
Notification en cas de brèche de données
(FTC et Règlement européen 2018)
3.
Droit à l'effacement
Encouragement aux codes de conduite
Droit à la portabilité des données
Légende:
1. Principes appuyés par 4 à 5 cadres (parmi FIPPS, OCDE, Directive européenne, Principes FTC, Règlement européen 2018)
2. Principes appuyés seulement par les cadres européens de 1990 et 2018
3. Principes appuyés seulement par le cadre européen de 2018
4. Principes appuyés par 1 à 3 cadres

Figure 3: Privacy Concepts Identified in Various Legal Frameworks

Many observers say that implementation strategies of government and business over the past few decades have underscored the importance of advice and consent. Protecting the privacy of persons concerned by certain data means: 1) Informing these people of the information practices of the entity collecting and using their data and, in particular, specifying what kind of data is collected and the reasons for its use. 2) Obtaining such persons' consent.[18] Data minimization and anonymization have also been proposed as privacy protection strategies.

[18] It should be noted that the advice and consent system has been heavily criticized for many years. For one thing, the notifications provided are at best difficult to read or understand and often perceived as non-negotiable terms for accessing the desired services. Consumers are also ill equipped to understand them (Viitanen and Kingston, 2013; Gaughan, 2016).

4.3 Urban IoT: Legal Framework in Crisis

Various aspects of Economy 4.0, such as installing of sensors in public areas, big data access and algorithm analysis, have triggered a crisis for the personal data protection strategies defined over the over the past few decades (Rubinstein, 2013; Crawford and Schultz, 2014; Narayanan, et al. 2016; Mantelero, 2014; Tene and Polonetsky, 2013; Gaughan, 2016). In the case of one urban IoT deployment, the following issues arose:

- Difficulty applying advice and consent rules to sensor-based data collection.
- Difficulty ensuring anonymization[19] of personal data in the presence of big data and predictive analytics.
- Generation of “personal” data.
- Difficulty promoting principles of proportionate allocation and data minimization in big data environments.

4.3.1 Advice and Consent in Disarray

The difficulties of letting people know their data is being collected by sensors and giving them a choice in the matter is well documented (Schaub, et al., 2015, p. 27). Sensors collect data from movements, emissions and processes within the city on a continuous, widespread basis, without any possible timeout to let people “click OK.” Furthermore, predictive data analyses, which generate unpredictable results, do not lend themselves to the concept of meaningful consent, which requires a statement of purpose at the start of data collection (Tene and Polonetsky, 2013).

4.3.2 Threat to Anonymization

Development of complex analytic techniques, accompanied by the proliferation of accessible, interoperable databases, facilitates re-identification of previously anonymous data (Ohm, 2010; Narayanan, 2016; Rubinstein, 2013; van den Hoven, 2012; EDPS, 2014; Gaughan, 2016). Advances in computer science, for example, have shown that people in a city can be identified with as few as four spatial-temporal data points (Montjove, 2013).[20] In a 2014 report, the US Council of Science and Technology concluded that it has become easier to reverse data anonymization.[21] Furthermore, the European Data Protection Supervisor noted that data generated by user activities is rarely completely and irreversibly anonymized (IERC, 2015).

[19] Anonymity is intended to eliminate the link between data and a specific person (Richards and King, 2004).

[20] Acquisti, Gross and Stutzman (2011) have also demonstrated that it is now possible to ascertain social insurance numbers using a photo of a person’s face. Appendix A gives such other examples as the scandal over re-identification of data released in 2014 by the New York Taxi and Limousine Commission (Tockar, 2014; Franceschi-Bicchierai, 2015).

[21] This “. . . could be used as a security measure, but it is not on its own capable of dealing with contemporary re-identification methods” (PCAST, 2014, pp. 38-39).

4.3.3 Proliferation of Personal Data

Contemporary data and technologies support the creation of new personal data. Data considered innocuous or anonymized in separate databases may become sensitive when those bases are merged (Crawford and Schultz, 2014; Metcalf, et al., 2016).[22] For example, retail giant Target used its customer database to create analyses identifying women who had recently become pregnant—even before they had shared this news with friends and family (Crawford and Schultz, 2014).

Such data amalgamation may be viewed as intrusive, whether or not it pertains to traditionally personal information (name and address, etc.). As Turow aptly states: “[i]f a company knows 100 data points about me in the digital environment, and that affects how that company treats me in the digital world, what’s the difference if they know my name or not?” (Turow in Barocas and Nissenbaum, 2014, p. 54).

In any event, even without collecting and using individual-specific data, inference and analysis can be used to assign characteristics to individuals that may be related to or identical with data considered personal. Such inferences can be made about a group if as few as 20% of its members provide information about their personal attributes (Barocas and Nissenbaum, 2015).

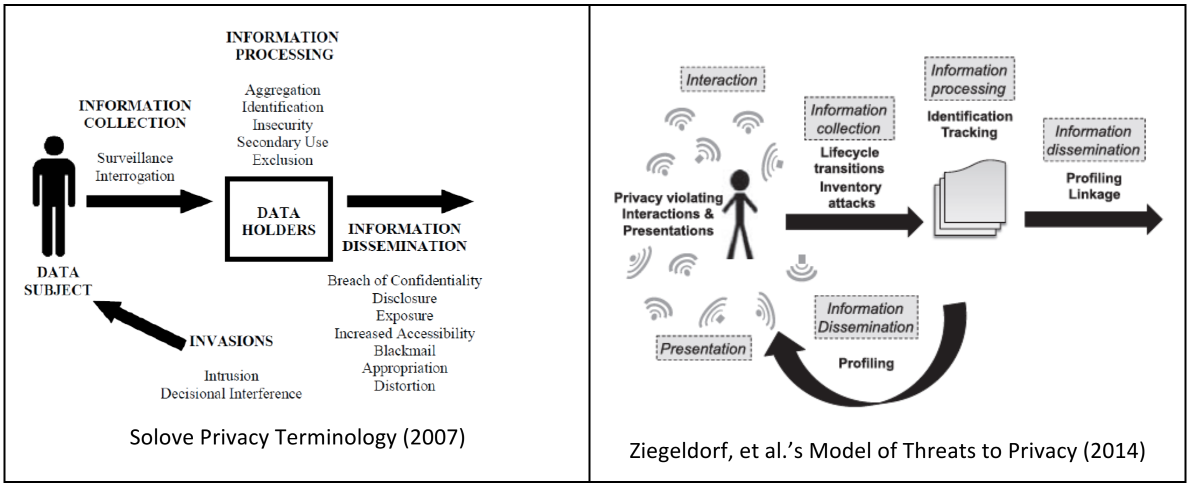
4.3.4 Data Minimization: Increasingly Less Relevant

Finally, the principle of proportionality—or minimized data collection and use—that is mentioned in several personal data protection reference frameworks (*FIPPs*, *OECD Guidelines*, *FTC Principles*, *EU General Data Protection Directive* and *Regulation*) has become increasingly difficult to enforce, while the potential for innovation offered by big data requires constantly increasing quantities of data (Rubinstein, 2013). The US Federal Trade Commission, in particular, believes that it is difficult to enforce data minimization (or notifications and opt outs), with IoT (FTC, 2015).

[22] Some writers refer to the concept of *personal public data*—all information not confidential in traditional legal terms, but that can still be linked to a person (Tavani, 2004; Nissenbaum, 1998).

4.4 IoT's Threats to Privacy

Many of the activities involved in rolling out an urban IoT system could raise ethical issues pertaining to privacy. The work of Ziegeldorf, et al. (2014) and Daniel Solove (2007) is particularly useful in identifying potential trouble spots. Ziegeldorf focuses on smart cities and Solove on privacy, generally. Appendix C takes a closer look at these works. As illustrated in Figure 4, the two authors identify possible threats to privacy involved in such activities as data manipulation (collection, processing and dissemination).[23]



Solove Privacy Terminology (2007)

Ziegeldorf, et al.'s Model of Threats to Privacy (2014)

Figure 4: Reference Models of Solove (2007) and Ziegeldorf, et al. (2014)

Based our research and that of the other writers we have consulted, we have presented a summary of threats to privacy[24] associated with these ethical issues, below. These threats pertain to three of urban IoT's four cornerstones:

- Data collection and storage.
- Data analysis.
- Data releases and services for the public.

[23] The authors identified other activities. Solove (2007) mentioned "invasion," which is not relevant to IoT. Ziegeldorf, et al. (2014), referred to interaction and presentation.

[24] These "threats" are activities, situations and contexts that could compromise privacy.

4.4.1 Potential Threats in Data Collection and Storage

This phase includes data collection, transmission, storage and archiving. Three threats to privacy have been identified at each of these steps:

- Data system security.
- Personal data collection without consent.
- The public's sense of being under surveillance.

Data and System Security

The exposure of computer systems to cyber and physical attacks has been widely reported (IERC, 2015; FTC, 2015; van den Hoven, 2012). A study commissioned by the European Parliament lists data breaches, malware infections, unauthorized access to personal data and illegal surveillance as such vulnerabilities (Euro Parl, 2015). The US Federal Trade Commission has named two principal weaknesses. The first is likely breaches of the central computing system that could give hackers personal information that has been stored in, or transmitted by a sensor, to it. Then there are in sensor security gaps that could facilitate attacks on the network to which the sensor is connected (FTC, 2015, p. 26).

The omnipresence of sensors in a connected city also amplifies vulnerability. Such sensors increase hacking opportunities, particularly as they often lack the capacity to contain sophisticated security systems and it is hard to detect attacks because they are so small (IERC, 2015). Writers have also noted that big data storage magnifies potential damage due to any data breach of sensors, servers or cloud storage (FTC, 2015).

Personal Data Collection Without Consent

Lack of information or notice about the collection and planned use of sensor data can heighten people's concerns that data is being collected without their knowledge. Many writers cover this issue in the literature, often with respect to the Internet of Everyday Things and online privacy[25] (Tavani, 1999; Barocas and Nissenbaum, 2014; Solove, 2007; Viitanen and Kingston, 2013).

Feeling Watched

The sense of being under surveillance during data collection may contribute to privacy concerns (Solove, 2007). Section 9 considers surveillance and its impact on freedom and personal identity in detail.

[25] In his classification scheme, Solove (2007) describes this issue in both the collection and data processing phases as an "exclusion." However, we believe the threat is only present during collection.

4.4.2 Potential Threats to Internal Decision-Making in Data Analysis

The following threats to privacy are present at this step:

- Personal profiles generated by merging data.[26]
- Personal profiles generated through re-identification.
- Personal profiles generated through profiling (inference).
- Geographic tracking of people.
- Data used for purposes other than those stated and intended.

Generating Personal Profiles and Geographic Tracking

As discussed in Section 4.3.3, it is more likely than ever before that personal profiles will be generated through cross-matching data and profiling (Section 5 examines the latter in depth). Ziegeldorf has also referred to the potential risks arising from personal geolocation.

Using Data for Other than Stated Purposes

While it is not easy to apply advice and consent requirements to urban IoT, harmonious deployment of such technologies implies some kind of public consent to the collection of data and its intended purposes. Data uses that are other than stated or clandestine have been mentioned as potential infringements of personal privacy.

4.4.3 Potential Threats of Releasing Data and Providing Services to the Public

For data to become open, it must be released by those administering it. Such data may then be examined, analyzed and used by third parties. Three threats are present at this stage:

- Distribution of confidential personal data.
- Distribution of data considered not confidential under the law, but which could affect someone’s reputation.
- Access to data that could contribute to the generation of personal profiles through data combination, re-identification and profiling.

It is clear that each data release increases the quantity of existing data and contributes to the likelihood that personal profiles are produced through data combination, re-identification and profiling by third parties.

[26] Includes Solove’s concepts of aggregation and identification, and Ziegeldorf’s of identification and linkage.

4.5 Potential Solutions

Privacy concerns pertaining to IoT and the smart city are complex. While the literature does not offer any miracle solutions, certain potential options have emerged, particularly with respect to technological, political and legislative remedies.

Several IERC teams have been created over the past few years to develop technical solutions to IoT security and privacy issues, including data confidentiality (through sticky flow policies[27]), metadata anonymization, user data anonymization, cyber-physical security, hardware authentication and equipment identity management. For more information on this initiative and others under development, see IERC, 2015.

4.5.1 Security and Privacy by Design

This approach, advocated by many writers and lead organizations, encourages system designers to incorporate security and privacy features in the development and construction of sensors and data processing systems (van den Hoven, 2012; FTC, 2015; Richards and King, 2004). Previously, such considerations were considered to fall within the exclusive domain of policymakers (Gaughan, 2016).[28]

4.5.2 Commitment to Non-Re-Identification

Anonymization is standard practice among European and North American regulatory bodies, although it is not considered adequate on its own.[29] The literature describes various solutions for overcoming the limits of anonymization, including organizational commitment to non-re-identification.

[27] Researchers funded by the European Commission are now seeking to apply sticky flow policies ensuring that access and confidentiality rules are associated, through metadata, with data flows. This includes the idea that each data point in a system is paired with a security policy defining how the data can be used and which conditions must be met before it can be migrated to a new data processing unit (IERC, 2015).

[28] Appendix A describes the main lines of this approach.

[29] In the *European Commission Directive on Data Protection 95/46/EC*, requiring that all data sources be anonymized or scrambled with a quantitative privacy guarantee corresponding to the likelihood of re-identification (van den Hoven 2012). The same rule has been applied on the other side of the Pond, with PCAST proposing anonymization as a strategy to de deployed, but which is inadequate by itself to protect data (PCAST, 2014).

In a 2015 report, the Federal Trade Commission recommended that businesses store their data in anonymized form (FTC, 2015) and implement mechanisms to ensure long-term de-identification. According to this approach, businesses should: 1) Take reasonable measures to de-identify data. 2) Publicly commit not to re-identify data. 3) Conclude binding contracts with third parties sharing the data, including the latters' commitment not to re-identify it (FTC, 2015).

4.5.3 Aggregate Data Collection and Data Minimization

Coarse-grain data gathering is another way to overcome the limits of randomization (van den Hoven, 2012). Gaughan (2016) gave the example of data collection systems that can be configured to aggregate data at the source, preventing local disaggregated data from being associated with individuals (Gaughan, 2016, p. 60). In many cases, aggregate statistics appear to meet the analytical needs of city governments.[30]

Finally, many frameworks are designed to minimize data collection and use, according to the principle of gathering only necessary data and keeping it merely for the time strictly necessary for analysis. This approach reduces the quantity of data that could be used to generate personal profiles and minimize vulnerability in case of a breach.

It should however be noted that aggregate and minimized data collection are strategies that run counter to the fundamental goals of urban IoT, as well as to one goal of an IoT project—collecting large quantities of disaggregated data, to promote subsequent reuse.

4.5.4 Differential Privacy Algorithms (DPAs)

DPAs generate "static" (small, quantifiable errors) in analytical results, making them "fuzzy," in contrast with results based on original data (Narayanan, 2016). As Narayanan explained, DPAs, like all data protection measures, represent a compromise between protecting privacy and manipulating data easily. The US Census Bureau employed this strategy to protect privacy in its OnTheMap program, as did Google for its RAPPOR (Randomized Aggregatable Privacy-Preserving Ordinal Response) initiative (Erlingsson, et al., 2014).

[30] Appendix A includes more information on these approaches.

4.5.5 Promoting Transparency and Potential Remedies

Several expects recommend focusing on how collected data is used and the decisions resulting from such use (Tene and Polonetsky, 2013), as well as on the data itself (European Parliament, 2015). This is particularly important where more traditional forms of consent do not apply and "other trust and trusted procedures have to be imagined" (IERC, 2015).

Drawing on Danielle Citron's (2010)[31] work on automated decision-making, Tene and Polonetsky (2013), Rubinstein (2013) and Crawford and Schultz (2014) have recommended that organizations be required to reveal the data used, criteria and inherent logic of their analytical process and procedures for making decisions using the collected data. The authors argued that such a requirement could discourage improper profiling and give people the opportunity to appeal decisions made by algorithm-based processes. This system would require entities that analyze data to produce an audit trail (Crawford and Schultz, 2014, p. 33).[32]

Transparency is also strongly recommended in data sales (Herschel and Miori, 2016). Furthermore, the principle of mandatory notification following a security breach has been introduced in the United States (FTC, 2015), and in the updated *EU Data Protection Regulation* (European Parliament, 2015).

Naturally, transparency is also recommended as a possible solution in Section 7 (Ethical Issue: Transparency and Reliability).

4.5.6 Defining Basic Principles of Data Collection and Use

Improving transparency in data collection and use means establishing guidelines on the topic. Such guidelines should be clear but flexible, to make way for the future evolution of technologies and perceptions (Harvard Law School, et al., 2017). Van den Hoven (2012) noted the importance of stipulating who can access which information, under what circumstances and for how long, as well as how the information can be used and combined with information from other data (Van den Hoven 2012). Some cities have begun setting basic universal privacy rules, particularly in terms of supplier relations[33] (Harvard Law School, et al., 2017). Seattle's initiative in this area is one example of that phenomenon.

Identifying basic principles is also a potential solution recommended in Section 6 (Ethical Issue: Separation of the Government and Business Spheres).

[31] Citron (2010) also suggested several supplementary measures that could be applied in this area, such as investing in unconscious bias training and mistakes in automated decision-making for employees using these decision-making systems (Citron, 2010). More information on Citron's recommendations can be found in (2010) Appendix A.

[32] Additional details on the *Procedural Due Process* approach recommended by Crawford and Schultz (2014) appear Appendix A.

[33] The report does not, however, state what these rules are.

Box 2: Seattle Privacy Principles (2015)

Following months of consultations with stakeholders, Seattle adopted six privacy principles in February 2015. They are:

1. We value your privacy: Privacy impact assessments will be conducted on all new data programs.
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, spelling out privacy and data management practices for all its departments. This commitment also requires a privacy impact assessment and a privacy threshold analysis for all new data collection programs (Gaughan, 2016).

4.5.7 Promoting Public Participation Through Data Use

Tene and Polonetsky (2013) advocate “sharing the wealth,” based on the idea of giving people access to their data in a useful, attractive format. Proponents of this approach believe that encouraging interaction between people and data is one way of bringing them on board the debate over data and their rights in this area. They also see this strategy as a way of promoting expansion of the data ecosystem, solutions and public apps, enabling people to analyze their own data and arrive at useful conclusions. As an example, the authors mention the Obama administration’s Green Button initiative, which gives consumers access to their own energy usage data in a user- and computer-friendly format (Tene and Polonetsky, 2013).

4.5.8 Formal Public Privacy Protection and Impact Assessment Body

A number of writers have supported the creation of a public privacy protection organization (Solove, 2007; Mantelero, 2014), similar to those now enforced in quasi-public and consumer protection organizations. Mantelero (2014) said that such an entity should have access to technological knowledge and a broad societal perspective to evaluate risks posed by data treatment/analysis, and balance the interests of different stakeholders that could be affected by large-scale data collection, extraction and analysis projects (Mantelero, 2014, p. 19).

Mantelero (2014) also recommended conducting multiple robust impact assessments on data processing, including the opportunity for people to opt out of certain analyses. It should be noted that privacy impact assessments have existed since the 1990s.[34] This new model, however, introduces the idea that organizations using big data must conduct an impact assessment of data protection and surveillance, as well as possible discrimination in the analyses and develop appropriate measures to minimize such discrimination. These assessments should be performed by third parties and supervised by data protection officials who would also be responsible for defining assessment criteria (Mantelero, 2014, p. 26).

4.5.9 Drawing on Research and Biomedical Ethical Principles

Research and biomedical ethical practices may provide useful frameworks for solutions. Barocas and Nissenbaum, for example, have proposed instilling ethical rules, much like a doctors' Hippocratic Oath, among scientific analysts and researchers. They also recommend using ethics review boards to evaluate data collection, use and dissemination programs (Barocas and Nissenbaum, 2014).[35]

The Council for Big Data, Ethics, and Society, consisting of 20 universities prominent in these social, natural and computer science disciplines, has formulated an ethics code based on *PLOS Computational Biology's* "Ten simple rules for responsible big data research" (Zook, et al., 2017). The first five concern minimizing potential damage caused by big data research and the remainder pertain to the use of best practices by researchers in their work (Zook, et al., 2017). The 10 rules appear in Appendix A.

4.5.10 Drawing on Traditional Privacy Frameworks and their Evolution

Several writers and stakeholders agree that traditional privacy principles are not completely applicable to contemporary IoT. However, some authors do agree that these principles could guide decisions in many ways and should simply be updated so they can continue to fulfill their purpose.

[34] The Federal Trade Commission, for example, recommends that businesses conduct security and privacy risk assessments (FTC, 2015, p. 44). The organization also recommends that businesses test their security measures prior to deployment.

[35] However, some writers see many limitations in this proposal, including the fact that data science as a whole (rather than a particular profession, such as medicine) employs a variety of tools in different contexts (private/public sector, etc.) (Gaughan, 2016, p. 53). Such a committee's authority could be compromised by a lack of legal remedies (such as licence suspension).

5 Ethical Issue: Social Inclusion

Many municipal actors contend that new technologies should be employed to reduce—not accentuate—social inequality (Harvard Law School, et al., 2017). Yet the inherent nature of IoT and the context of its deployment indicate that there are many hurdles to overcome before achieving these goals. Furthermore, our literature review underscores multiple ethical issues pertaining to social inclusion.

Box 3: Discrimination

This section covers the concept of discrimination—attitudes based on stereotypes and prejudices.[36] Ambrose Bierce[37] defined prejudice as “a vagrant opinion without visible means of support.” In other words, prejudice is a groundless assertion. Stereotypes are rudimentary descriptions and rigid simplifications used to characterize a thing or person. They are all embracing, prefabricated, social and used in a virtually automatic or routine manner (Moscovici, 2014).

Stereotypes and prejudices are used to describe the world in an oversimplified way, by overstating similarities between members of a particular group and differences between groups. Please see Appendix D for further information on this subject.

5.1 IoT’s Threats to Social Inclusion

Possible threats[38] to social inclusion may occur in all four phases of urban IoT:

- IoT project planning.
- Data collection and storage.
- Internal/external data analysis.
- Releasing open data and providing services to the public.

[36] Stereotypes and prejudice are two expressions of a collective characterization that defies analysis and focuses on describing others (Amossy, 1989).

[37] *The Devil's Dictionary* contains ninety-eight satirical definitions written by Ambrose Bierce from 1881 to 1906.

[38] These “threats” are activities, situations and contexts that put privacy at risk.

5.1.1 Possible Threats in IoT Infrastructure Planning and Maintenance

Two threats to social inclusion have been identified at the IoT technological infrastructure planning and maintenance phase:

- Channelling investments toward IoT rather than to other urgent urban issues.
- Geographically unequal investment.

A concentration of resources in the smart city project, accompanied by the widespread use of smart city rhetoric, promoting the concept as inherently beneficial, apolitical and thus essentially beyond criticism—has served to channel massive public investment toward IT rather than to other necessary action areas (Söderström, 2014). For this reason, multiple stakeholders have condemned the failure to address such high-priority urban problems as property prices, social harmony/relationships between different communities, and retention of local services, etc., in rolling out the smart city as a service (Kaplan, 2012). In the case of the smart city, special emphasis has been placed on changes in such areas of governance as energy, transportation and technology—to the detriment of others (Felli, 2015).

Concentrations of funding, infrastructure and policies are also shifting geographically, with some urban districts benefitting to the detriment of others (Felli, 2015). De Breux and Diaz (2016) also noted that studies on such self-proclaimed smart cities as Singapore, Rio de Janeiro and Boston, present a more mundane situation, where urban intelligence is confined to a few small districts and certain sectors of governance. The same rules apply to nearby suburbs, which are often excluded from such technical and social projects, increasing the social gap between communities (Felli, 2015).

Finally, some writers say that a major project of this kind would obfuscate the slight progress of other urban planning goals, as well as controversies over actual benefits of certain value-added projects (Douay and Henriot, 2016).

5.1.2 Potential Threats to Data Analysis

One threat to social inclusion has been identified at this step:

- Discriminatory profiling by algorithms.

Many studies refer to **the potentially discriminatory effect of algorithms**. Romei and Ruggieri (2013) have established a comprehensive inventory of the vast number of discrimination surveys involved in data production and analysis. Their article identifies and describes a variety of pitfalls that have not only skewed the production of scientific data, but reinforced existing forms of bias. Furthermore, they mentioned that algorithmic software employ stereotypes and prejudices. In many cases, such apps even serve to amplify social, legal and economic discrimination (Sweeney 2013; Barocas and Selbst 2015; Birrer 2015; Winter, 2015), often resulting in unfair treatment of individuals, based on their profiles (Goodman, 2016).

Algorithms classify and simplify information according to their programmed values. They are designed to accentuate similarities between members of a particular group, as well as differences between preconceived categories. This means algorithms are inevitably “embedded with values” defined by developer operating parameters and as configured by users (Mittelstadt, 2016) , as well as through possible discriminatory bias present in data, which often reflects existing social stereotypes. Poor quality data can also create algorithmic bias.

Box 4: The Example of COMPAS Software

American judges use the COMPAS algorithm[39] in sentencing. To determine its effectiveness, ProPublica (Larson, et al., 2016) compared the sentences of 10,000 people arrested in Broward County, Florida, with the algorithm’s predictions, while they were detained in 2013 and 2014. The journalists counted the number of previous defendants who were rearrested over the subsequent two years. The large number who were clearly illustrated ethnic discrimination. African Americans were twice as likely to be incorrectly perceived as potential violent repeat offenders. Whites who re-offended and had previously been charged with violent crimes were 63% more likely to be incorrectly assigned a low likelihood of violent re-offensive with respect to a black criminal having the same profile.

5.1.3 Possible Threats from Data Releases and Services for the Public

Four threats to social inclusion have been identified at this step:

- Limited access to data and services, due to the digital divide (those not able to access or understand the data).
- Lead role for the public in using open data impossible or limited.
- Limited urban access for disenfranchised target groups.
- Unequal access, depending on digital user profile.

Unequal Access Due to the Digital Divide

As previously mentioned, the urban IoT project aims to improve services to the public, notably through development of effective online services (including apps) and open data, which could stimulate the creation of new studies and services for and by the public. Under these circumstances, maintaining telephone-based and face-to-face services is important for groups with less Internet access, in view of current progress in enhancing online services.

[39] *Correctional Offender Management Profiling Alternative Sanctions*.

Giving the public access to upgraded municipal digital services presupposes that it can understand these technologies and the information they provide and use them to improve their quality of life (Poty, 2014). These services, in short, are only accessible by individuals with reading,[40] numeracy[41] and problem-solving skills suited to technology-rich environments (PSTRE).[42] This "digital divide" constitutes a major challenge to social integration (Rallet and Rochelandet, 2004; Mossenburg, et al., 2003). That issue dovetails with and can reinforce existing traditional (wealth), demographic, territorial and educational social divisions (Peres, 2015).

The digital divide is present in Montréal and throughout the rest of Québec. According to data from the Institut de Statistique de Québec, about one in five Quebeckers has poor literacy and numeracy skills.[43] Furthermore, 51% of the population has poor to very poor Internet skills. Finally, 16.4% of Montréal households had no Internet connection in 2012 (Institut de la Statistique du Québec, 2015).

Such difficulties accessing municipal services generate inequality: "Those with limited access either pay with time lost trying to use these services or in going to speak with someone directly. A worse scenario is simply not using certain services out of frustration" (Conseil national du numérique, 2013, p. 78). Furthermore, reduced access to services and information available to "the others" creates a sense of exclusion, worthlessness and powerlessness among disenfranchised groups (Plantard, 2013).

[40] The ability to understand, assess, use and make commitments in texts, to play a role in society, achieve personal goals and develop personal knowledge and potential (OECD, 2014, p. 20, in ISQ, 2015).

[41] The ability to find, use, interpret and communicate information and mathematical concepts to deal with the mathematical requirements of many situations in adult life (OECD, 2014, p. 20, in ISQ, 2015).

[42] Using digital technologies, communication tools and networks to acquire and evaluate information, communicate with others and perform practical tasks (OECD, 2014, p. 32, in ISQ, 2015).

[43] "Poor" literacy or numeracy means an "inferior" skill and "Level 1" of the ISQ Scale. In the case of PSTRE, "very low level" means "inferior" and "low" means "Level 1" of the ISQ Scale. Please see Appendix F for further information.

Limited Access to Lead Role Using Open Data

Only those individuals with solid literacy, numeracy and PSTRE (Problem Solving in Technology Rich Environments) skills will, at least over the short term, be able to play important roles in using open data for analysis, enriching democratic debate and developing new apps. Such roles not only require an understanding of and a control over basic technologies, but the ability to analyze data and develop programs. This means revising the concept of digital divide beyond the current narrow focus on user skills, while considering the importance of being able to analyze and use data.

Few Municipal Services for Disadvantaged Groups

Because of their difficulty accessing online services, digitally marginalized groups have less chance of getting their needs to rank highly among newly created services (Viitanen and Kingston, 2013). Such needs pertain to technology and content. Technologically, the vast majority of online services are designed for an audience with functional literacy, numeracy and PSTRE skills—rather than those at the bottom of the learning curve (Santa Clara University, 2017). In terms of content, the development of services targeting a digitally literate audience is bound to disregard the special needs of disenfranchised groups. This is all the more important in view of overlaps between digital disenfranchisement and of other social determinants of marginalization (education, wealth, demographics, etc.). That means two forces are at work accentuating urban socioeconomic disparities (Viitanen and Kingston, 2013), with services provided in a format inconsistent with personal abilities and poorly equipped to meet special needs.

Unequal Access for Different User Profiles

Algorithms employ the digital tracks people leave, knowingly or not, in most apps they use. A vast array of algorithms use data tracks (words, sounds, images, numbers, descriptors) to channel consumers toward new markets (recommended products, services and organizations). This results in both discrimination and isolation, since users, depending on the tracks they leave—that are a function of their social class, inquisitiveness and education—will have very different opportunities, which in turn tend to reinforce their own discriminatory biases.

Box 5: Will the Smart City be a Ghetto of the Rich?

Inclusion is the focus of various social movements. On February 8, 2017, Ouishare organized a round table on “SMART CITIES DON’T LIKE THE POOR,” which took the position that smart cities “will become a ghetto of the rich.” The Ouishare community, in response, supports public ingenuity and recommends replacing the marketing posture of “Smart” with the concept of “shared city living.”

Box 6: Public Participation, by Civic Tech

In Canada’s English-speaking cities, led by Toronto, the term “Civic Tech”[44] is the umbrella term for all of a municipality’s public technological initiatives. Using shared or open-source data, apps are created for use by the public. For civic technology proponents, these apps constitute a sea change in the public participation model by emphasizing the “logic of action.” The announced intention of representatives of the international and urban Civic Tech movement is to give power, in addition to the vote, back to the people. Civic Tech is making city-dwellers true stakeholders in the common good.

5.2 Potential Solutions

The literature and interviews identify the following potential solutions for alleviating ethical issues of social inclusion:

- Emphasizing education and access to information technologies.
- Getting residents on board, by focusing on municipal goals rather than technology.
- Making digital literacy a policy challenge.
- Developing universally accessible and useful services.
- Developing open, transparent algorithms.
- Developing algorithms that comply with certain ethical principles.
- More effectively including external partners (media and advocacy groups) that are engaged in the dissemination of information.

5.2.1 Education and Access to Information Technologies

A number of observers advocate support for digital education (Peres, 2015). These proposals include:

- Promoting access to broadband technologies and Internet.
- Helping families teach children and young people.
- Promoting continuous learning in schools, kindergartens and higher education.
- Supporting deployment/enhancement of Wi-Fi access points and education for adults who are no longer in school.
- Promoting basic literacy/numeracy skills—the foundations of digital education.

[44] http://civictech.ca/

Many have recommended that digital education focus on a range of technologies, rather than merely learning apps, while encouraging critical, informed use of technology (Peres, 2015; IERC, 2015), accompanied by creative and productive skills. It has also been suggested that students be introduced to three basic IT concepts: language, information and algorithms (Conseil national du numérique, 2013).

In terms of installing new and reinforcing existing Wi-Fi access points and providing education, support networks have been proposed that take into account the ongoing education required by a constantly evolving environment (Conseil National du Numérique, 2013). Digital education will also benefit from not merely being perceived as way of “catching up,” but as training geared to the development of creativity, along with personal and collective growth.

5.2.2 Uniting People Around Goals, Rather than Technology

In view of the digital divide and varying levels of public engagement, the smart city’s collective goals should be shared to support broad-based social inclusion. In other words, social inclusion should not depend solely on digital numeracy, but on the ability to understand, discuss and improve the IoT project, and ultimately participate fully in it, in full knowledge of the facts.

5.2.3 Digitally Supporting the Public’s Political Power

Daniel Kaplan (2012) suggested making the city not just a distributor of information, but of power. The new partnership of city government, business and residents that the smart city offers is not necessarily limited to “opening data,” but to facilitating pioneering concepts that can increase social harmony. According to Kaplan, there are abundant examples of such ideas: “mobilizing neighbors and shopkeepers to help seniors restore Wi-Fi access, where it has disappeared, to public and private services, sharing expensive, underused equipment . . . recycling and providing transportation for poorly served neighbourhoods.” (Kaplan, 2012). The smart city should accordingly provide resources for putting data into the proper context and tools for taking such actions as “creating programming interfaces on certain municipal apps (fee calculation, mapping, etc.), organizing tools and giving presentations, etc., to facilitate use of these resources by unspecialized players; training these unspecialized players to help them empower themselves; open meeting, coproduction and mutual assistance facilities, and showcasing activities supported by digital tools” (Kaplan, 2012).

Others also emphasize the profoundly political role of e-inclusion. To be truly included in a political project aimed at achieving social harmony, people must not only be members of society, but be engaged as stakeholders in terms of their social bonds and contributions to economic and cultural life. While many such interactions are now digital, skills in supporting this kind of social inclusion are also necessary. This means the technical aspect of the digital world must be repoliticized (Conseil National du Numérique, 2013). In other words, a technological project should not be perceived as nonpartisan and apolitical, but rather as central to the democratic process. Such a project should also be perceived as embodying values and contributing to the reinforcement or reconfiguration of our society’s power relations.

Public participation in the IoT project is a subject discussed in several of the potential solutions presented in this report, particularly in Section 4 (Ethical Issue: Privacy) and Section 9 (Ethical Issue: Privacy).

5.2.4 Accessible and Relevant Services for All

As described above, digitally marginalized groups have less chance of getting their needs to rank highly among newly created services (Viitanen and Kingston, 2013). Such needs pertain to technology and content. Technologically, the vast majority of online services are designed for an audience with functional literacy, numeracy and PSTRE skills—rather than those at the bottom of the learning curve. Disenfranchised groups should be included at the design stage to increase the likelihood of meeting their specific needs. Governments also have an important role to play in developing platforms that provide public access to data sets.

5.2.5 Algorithmic Accountability[45]

Some writers advocate *algorithmic accountability*, which means making algorithms *auditable* (Sandovig, et al., 2014). However, this approach has been criticized by such writers as Antoinette Rouvroy and Bernard Stiegler (2016), who explain that making an algorithm's workings visible does not mean it can be understood or validated.

According to Cardon (2015), accountability makes an algorithm more robust by emphasizing its didactic aspect, requiring its creator to make what the algorithm does comprehensible. An algorithm is accountable because it provides constant assurance that it does what the designer said and the designer said what the algorithm does. The audit mechanism tests the algorithm's results. It might be noted that the Turing Institute's Suchana Seth (2017) is currently studying algorithmic accountability and the possibility of incorporating ethical codes in algorithms.

5.2.6 Ethics in Design

The IERC (2015), on the other hand, advocates ethics in design—making players aware of the process that will incorporate values and standards in algorithms—to make these value selections visible and transparent. This approach is ultimately intended to incorporate recommended values and rights in algorithms (IERC, 2015).

[45] For further information on algorithmic accountability, see Christine Balagué, "Plaidoyer pour la loyauté des algorithmes," *Éthique de la recherche en numérique. Gouvernance des algorithms*, Feb. 2016, Paris, France. 2016. <hal-01274665>

5.2.7 Discrimination Aware Data Mining

These proposed technical solutions are based on Discrimination Aware Data Mining (DADM) (Pedreschi, et al., 2009). The idea is to eliminate the black box in algorithms and prevent the risk of discrimination. For DADM's authors (Asmita Kashid, et al., 2017), this involves creating a digital app that would: (1) Audit the algorithm to quantify its discriminatory potential. (2) Provide an explanation of the rules governing data collection and analysis. (3) Explain the mechanisms used to mitigate discrimination. Individuals and the community will welcome quantification of an algorithm's discriminatory potential.

One question arises, however. Can the realignment of relationships between individuals and organizations be limited to software tweaks?

5.2.8 Regulating What Algorithms Can and Cannot Do

Various attempts to establish a legal framework for algorithmic analyses are emerging. The European Union, for example, has decided to regulate the issue of discriminating algorithms (Goodman and Flaxman, 2016). On April 27, 2016, the European Parliament validated the regulatory framework of the new *EU General Data Protection Regulation* on data production and analysis, to ensure personal privacy and prevent algorithmic bias (European Parliament, 2016).

Other writers recommend defining the *rules of the game*—what an algorithm can or cannot do. Goodman and Flaxman (2016) suggested setting up testing agencies to determine if an algorithm does what it is said to do. They also recommended developing a set of rules applicable to all designers (Goodman and Flaxman, 2016). On May 30, 2017, Ben Shneiderman[46] proposed to the prestigious Alan Turing Institute of London the creation of a National Algorithm Safety Board, modelled after transportation boards. The notion of control mechanisms is clearly making headway.

[46] https://www.turing.ac.uk/events/turing-lecture-algorithmic-accountability/

6 Ethical Issue: Separation of the Government and Business Spheres

Urban IoT poses ethical issues pertaining to separation of the government and business spheres. As discussed in the Introduction to this report, the Smart City Project has, from the start, been strongly promoted by private interests, such as Internet and communications technology (ICT) firms (Carlsson, 2014; Kaplan, 2012; Greenfield, 2014). At the present time, IoT equipment, hardware and software for the smart city are mostly supplied by the private sector, which has the required know-how for developing these leading-edge devices. Furthermore, a project involving the release of certain data to the public also implies significant private sector involvement in analyzing and mobilizing data used in the creation of apps for the public and the private sector. Open data, of course, is also intended for use by public entities, media and the public. However, it seems likely that the private sector will be at the head of the queue to exploit this new data windfall.

The strong influence on the smart city of private players could undermine the separation of the government and business spheres, posing ethical issues. Édith Deleury, former president of the Commission à l'éthique en sciences et technologies du Québec (CEST), is concerned about how the private sector is acquiring growing control over municipal data and services (Deleury, 2016).

6.1 Potential Threats to Separation of the Government and Business Spheres

Possible risks to the separation of the government and business spheres pertain to three of the four main phases of Urban IoT:

- IoT infrastructure planning and maintenance.
- Data analysis.
- Open data and services for the public.

6.1.1 Potential Threats to Planning and Maintaining IoT Infrastructure

At the IoT infrastructure planning and maintenance phase, three possible risks to separation of the government and business spheres have been identified:

- Shaping the smart city project around private interests.
- Locking-in the project technologically.[47]

[47] The linking of cities to technology platforms or vendors over long periods creates monopolies (Deleury, 2016; Kitchin, 2014b; Angelidou, 2015; Hill 2013).

Shaping the Smart City Project Around Private Interests

Rob Kitchin (2014b) believes smart city governance is usually coopted and explicitly shaped by private interests for their own benefit (Kitchin, 2014b). Technology remains the key to the smart city designs and visions of such firms as IBM, Cisco Systems, Siemes AG, Nokia, Veolia, Dassault, General Electric, and Philips, etc. (Albino, Berardi and Dangelico, 2015; Douay and Henriot, 2016). Smart city projects are themselves characterized as apolitical—as solutions not driven by ideological interests, but by "common sense" and optimization objectives (Koolhaas, 2014; Oddoux, 2016).

Under these circumstances, many observers are concerned that municipalities will turn to off-the-shelf products, rather than engaging in detailed assessments of resident needs and requests (Deleury, 2016). Kitchin (2016) says that private businesses sell cities solutions that ignore their historical, political, social, territorial and cultural contexts. Evgeny Morozov (2015) calls this approach *solutionism*, meaning that the private sector provides an overly narrow definition of social problems and does so in terms that will primarily benefit the "solution's" developers (Morozov, 2015b).

This was also the position of municipal representatives at a Harvard Law School international workshop,[48] who observed that businesses that vend their services will primarily promote their own agendas, rather than seeking to improve resident quality of life (Harvard Law School, et al., 2017). "We're often finding that there's a gap, sometimes quite a large gap, between the way that vendors approach us and the kinds of challenges that we want to take on," they said (Harvard Law School, et al., 2017).

Locking-In the Project Technologically

Government dependence on a limited (sometimes very limited) number of businesses acting as the principal technology providers poses a threat to free policy-making by governments, along with their resilience and flexibility. It is rarely useful for businesses to create and sell technologies that will be easily compatible with equipment and software supplied by other vendors. Furthermore, the many updates required for proper operation of the equipment, the difficultly for users to make changes and technological rigidity bolster the power of private companies—along with government dependence on them (Deleury, 2016). Some cities, incidentally, are entirely governed by private firms, including Masdar City in Abu Dhabi and Songdo International Business District in South Korea (Kaplan, 2012).

[48] Organized in 2016 and attended by representatives of 17 cities, mostly in the US but from other nations, as well.

Then there are equipment and service contracts that pose issues of pricing and terms. Many municipal stakeholders, for example, point to the sometimes-astronomical prices of various services, as well as the many vendors interested in providing their services condition on the right to resell data acquired through these services or to use the data for commercial profiling (personal communication).

In this context, government officials quickly become dependent on devices developed (and sometimes controlled) by businesses. Local governments can quickly be disempowered by digital experts and companies exploiting big data (Felli, 2015).

6.1.2 Potential Threats in Data Analysis

Two threats to separation of the government and business spheres have been identified at this step:

- Development of enhanced services for the "public" controlled by business.
- Growing dependence on selling data to generate revenue.

Development of Non-Public Services with Growth-Generation Potential

In the case of Montréal, the hope is that the private sector's mobilization of open data and app development will bring innovative solutions to urban issues. However, since many services created in this manner are paid and controlled by private businesses, some observers have put the public on guard. As Morozov (2015) wrote, passing some responsibility for service creation to businesses that produce paid apps reduces access to certain services intended for wide-scale use and that serve as add-ons to services generally considered to fall within the municipal sphere.

By taking this approach, cities are shedding their ability to administer or organize services (pertaining, for example, to urban mobility), as they would prefer (Morozov, 2015). They also risk becoming dependent on these new private services, which could become critical, although their commercial functions make not be aligned with municipal goals.

This process of service creation and enhancement by private business also corresponds with a reduced role for and less involvement by government (Oddoux, 2016). Such a situation can heighten the perception that city government is abandoning one of its fields of jurisdiction.

Dependence on Income Generation

Data is central to the urban IoT project. Some describe data as a resource, others as a new form of currency (Berthier and Kempf, 2015). One thing is sure: there is now a big market for selling and reselling data. Providing access to data and leasing infrastructure can generate income for the government, through profit-sharing or sale (Harvard Law School, et al., 2017).

Some cities have developed civic data exchanges where businesses can obtain high-quality data (comprehensive, frequently updated, etc.). A few cities are exploring the possibility of releasing high-quality public data to such platforms, while providing data of slightly lower quality[49] to open data exchanges. Income generated is then used to fund the smart city project (Harvard Law School, et al., 2017, p. 10).

Under these circumstances, the pressure on governments to generate revenue is high and can steer projects away from the public interest.

6.2 Potential Solutions

6.2.1 Controlling the Technology and Administering Partnership Terms

To offset the private sector's influence, cities are encouraged to set clear partnership conditions with suppliers of these technologies and control the IoT system, as much as possible. In so doing, cities should:

- Establish and communicate a clear idea of project requirements and values.
- Generate data on its own, to the extent possible.
- Retain ownership of the data.
- Encourage competition among vendors.

6.2.2 Establishing/Communicating a Clear Idea of Project Requirements and Values

Many municipal representatives have emphasized the importance of identifying public needs and values intrinsic to the IoT project, in shaping it. This approach provides a government with criteria for guiding the development of infrastructure, along with data processing and analysis, in line with the public good.

Many municipal representatives also underscore the importance of staying focused on municipal needs, with technology not an end in itself but a way of meeting the city's goals. They note the importance of learning to say no to vendor solutions that are not tailored to such goals (Harvard Law School, et al., 2017).

Educating and training vendors on this topic is essential (Harvard Law School, 2017). Some cities invite businesses to their offices to explain specific needs and determine which can be met by existing solutions or through the development of new products. This approach can turn a sales relationship into a partnership and expand the range of products or services offered by the vendor.

[49] Such lower quality does not means the data is poor. Rather, it refers to sound data that lacks some features of high-quality data, such as frequent updates.

6.2.3 Generating and Owning Data

Experts have also discussed the importance of a city generating its own data and maintaining ownership of it. Morozov (2015) said that cities should try to generate the data they need for their own management and then decide if they do or do not want to permit private firms to use it and under what terms. New York and Chicago, for example, are trying to launch a central app for dispatching conventional taxis with the ease of Uber. In addition to contending with Uber's market domination, the program will prevent trip data from becoming a costly commodity that city governments must purchase at high prices (Morozov, 2015).

Box 7: Cities at the Wheel of Innovation

Some cities have rolled out apps to inform residents of all transit options, from self-serve bikes on the corner, to minibuses with itineraries tailored to passenger needs.

Helsinki, in partnership with the Ajelo start-up, created Kutsuplus, a cross between Uber and a traditional transit system. "Passengers request a shuttle on their phone and the app calculates the best way of getting everyone to their destinations, using real-time data. It also provides an estimate of travelling time, by Kutsuplus and other forms of transportation" (Morozov, 2015b).

Such a project can only be successful if cities look beyond existing solutions. Considering Uber to be the only way of boosting the efficiency of public transit and reducing traffic jams is not the best starting point. Morozov also suggested that struggles over providing services to the public will be won by those owning the data and the sensors that generate it. "By leaving all of that to Uber—or worse, to giant hi-tech firms seeking to capture a share of the lucrative "smart city" market, cities are passing up the chance to conduct experiments that would enable communities to organize their transportation systems as they see fit" (Morozov, 2015b).

In short, "It is not become Uber comes from California—a region famous for poor public transit—that we should think personal motor vehicles are the future of transportation" (Morozov, 2015b).

6.2.4 Breaking up Monopolies

One way of ensuring greater control over urban technology is to keep private firms from acquiring a monopoly over it. The vast number and types of vendors give the city more freedom and let them maintain a central role as project overseer (Pouilly, 2014). This approach also lets the city take an innovative approach to harmonizing hard- and software supplied by different vendors within the project—yielding a far more resilient architecture.

7 Ethical Issue: Transparency and Reliability

Deploying IoT technology in the smart city and analyzing the data it generates raise ethical questions of transparency and reliability. These issues apply to three of urban IoT's four steps:

- Data collection and storage.
- Data analysis.
- Open data and municipal services.

7.1.1 Potential Threats in Data Collection and Storage

One threat to privacy has been identified at this step:

- Data system security.

Data System Security

System security is an important issue in terms of the credibility and reliability of a system like IoT in the smart city. Section 4.4.1 discusses the vulnerabilities mentioned in the literature. In terms of system reliability, it should be noted that highly automated and interconnected systems (particularly industrial ones) are at greater risk of being hacked (American International Group, 2016). In the case of a connected city, hacking could immobilize the operating and decision-making processes residents need for crucial services. The crashing or hacking of automated systems also raise questions of liability, while underscoring the social, environmental and economic impact of such problems. In other words, these potential issues pertain to daily living, as much as to public safety.

7.1.2 Potential Threats of Data Analysis

One threat to privacy has been identified:

- Lack of transparency of technological systems and analyses.

Opacity of Systems and Analyses Used

The complexity and lack of transparency of current data analyses and systems directly affect people's right to know what will be done with their data (European Parliament, 2015). The public has only a foggy notion of the kinds of data collected, how this is done, why it is analyzed and the kind of technology concerned. Furthermore, big data analyses often include data analysis for purposes other than those specified during collection (European Parliament, 2015).

Some observers, however, say that extensive communication with the public on the analyses performed and the system architecture would create additional security risks for systems or individuals trying to game the system by such means as generating false data through their activities or by computer. There is a fine balance, in other words, between the desire to open data and the need to refrain from saying anything, particularly in view of public security (Richards and King, 2014).

7.1.3 Potential Threats of Open Data and Services for the Public

One threat to reliability has been identified at this step:

- Quality of generated and open data.

Quality of Generated and Open Data

Data must be of high quality to ensure that it can confidently be used in decision-making (Lee, 2017). However, open data released by government agencies is not perceived to be high in quality (personal communication, 2017). The work of McArdle and Kitchin (2014), drawing on their experience as developers of applications employing urban data, highlights the difficulty in evaluating data accuracy without quality reports from data providers (McArdle and Kitchin, 2014, p. 1).

The authors noted that open-data portals usually do not include enough metadata to let users assess data quality (p. 9). A study of data portals in London, Paris and Dublin reveals that no information on general or specific quality measures accompanies their data. While some data tracking elements, such as the data's age and its supplier's name, is shared, the process of transforming the data from a raw commodity to a finished product is not described (McArdle and Kitchin, 2014, p. 9). More often than not, open data is provided "as is," with no assurance as to its accuracy, continuity of traceability.

McArdle and Kitchin warn that if government agencies fail to deal with data accuracy issues, open-data portals may be perceived as potential "dumping grounds for unreliable, unaudited and poorly preserved data" (McArdle and Kitchin, 2014, p. 9). The authors acknowledge that the ultimate problem is rarely lack of interest by officials, but inadequate resources.

7.2 Potential Solutions

Crowdsourcing to Increase Metadata

McArdle and Kitchin (2014) argue that, in the absence of data providers using metadata and user manuals to document their data quality, open-data portals should employ a crowdsourcing mechanism to generate and record user feedback and tweaks to improve the quality of data from urban sources and open government portals (McArdle and Kitchin, 2014, p. 1). This would permit subsequent work by others, with errors detected, and problems with or uses of the data shared in the same manner as with volunteer geographic information (VGI) systems.

Monitoring Data Quality with Metrics and Standards

A variety of guidelines and measures have been proposed to define data quality rules to observe (Batini, et al., 2009). ISO data quality standards have been developed, including ISO 19115-1:2014 (Geographic information — Metadata) and ISO 19157:2013 (Geographic information — Data quality). McArdle and Kitchin also refer to the work of the International Cartographic Association, which has identified seven metrics associated with the accuracy of spatial data.[50] They also mentioned work on transportation by the scientific community, which found ways of disclosing traffic data quality (Turner 2002 in McArdle and Kitchin, 2015).

The US Environmental Protection Agency (US EPA) has selected four questions to answer when publishing environmental data, to permit users to assess the quality of this data and determine if it corresponds with its intended purpose (US EPA 2006). These questions appear in Appendix D.

Then, there is the Open Data Institute, which created the Open Data Certificate to enhance the credibility of data supplied by data providers. Suppliers auto-certify by answering a set of questions about their data. A description of their quality control procedure is submitted with the data to obtain certification (ODI, 2015). The EU INSPIRE Directive also requires that geographic and tracking metadata be provided along with the data itself (Inspire, 2015).

7.2.1 Building Trust Through Transparency

Transparency can play a key role in building trust between residents and government agencies. It can also be instrumental in preventing abuses of institutional power. Transparency permits healthy checks and balances within government and between the government and governed (Richards and King, 2014). Some stakeholders and experts have identified ways of building trust through transparency, including:

[50] "*Lineage, positional accuracy, attribute accuracy, completeness, logical consistency, semantic accuracy, temporal data*" (Guptill and Morrisson, 1995, in McArdle and Kitchin 2015).

- Gradual deployment: start slowly, limiting data collection, and take the time to explain new projects to the public.
- Be clear on what data is not collected.
- Clearly explain key analytic operations, goals and subsequent manipulations of the data collected, and identify any third parties involved, while allowing for future adaptability and evolution.
- Clearly identify what data is considered sensitive (personal, geolocation) and how it will be handled.
- Let people know what the city has already done or implemented (Harvard Law School, et al., 2017; European Parliament, 2015).

Available channels of communication and information technologies can be used to provide such information. However, one-on-one human interaction is fundamental to building trust between the public and government agencies and should not be neglected. According to various municipal representatives, such interaction is essential to the success of long-term initiatives (Harvard Law School, et al., 2017, p. 12).

Section 4 (Ethical Issue: Privacy) also identified transparency as a possible solution.

8 Ethical Issue: Freedom

The deployment of urban IoT poses ethical issues pertaining to personal freedom, autonomy and self-determination. These issues are associated with two of the four phases of urban IoT:

- Data collection and storage.
- Data analysis.

8.1.1 Potential Threats in Data Collection and Storage

Two threats to freedom have been identified at this step:

- Actual or perceived universal surveillance.
- Greater dataveillance due to the enhancement of available data.

Actual or Perceived Universal Surveillance

Deploying an Internet of Things is accompanied by transparency and the release of data that can empower the public through such means as permitting examine its environment and the actions of city hall more closely, as well as by developing local solutions to problems. However, an environment crammed with data sensors can have a muzzling effect on the public, whose words and actions are constantly being converted to digital code.

According to psychological and psychoanalytic thinking, constant subjection to observation, scrutiny and examination can trigger a "suspension of identity" (Birman, 2011, 40). People who are constantly under watch feel like prisoners of an omnipresent "gaze" and seek to break free of it. It has been shown, for example, that surveillance has an impact on self-censorship and censorship of minority opinions (Richards, 2013; Stoycheff, 2016). Such surveillance consequently has an impact on freedom of expression and thought—core principles of a free society and of most theories of democratic political freedom (Richards, 2013, 1951).

Box 8: The Panoptic City

Many writers recount Bentham's Panopticon metaphor to describe the kinds of problems resulting from ubiquitous surveillance. The Panopticon is a circular prison with a watchtower where a guard may be present, but who cannot be seen from the outside. The tower faces many cells of prisoners. The inside of every cell can be viewed from this tower. The main effect of the Panopticon is to make inmates feel as if they are constantly under surveillance. This ensures that power over them is automatically maintained. The effects of such surveillance are relentless, even if such monitoring is not. Perfect power tends to make its application unnecessary . . ." (Foucault, 1975, p. 234). The power (watchtower) is always visible, but prisoners cannot be sure if anyone is actually watching them, although they know they could be under observation at any moment. The same inductive logic applies to connected objects. Their sensors reap vast quantities of data, but people do not know in advance what will be seen. Rob Kitchin writes that deploying urban IoT could potentially create a *panoptic city* (Kitchin, 2014)[51].

Increasing Dataveillance to Enhance Available Data

"Dataveillance" is a form of surveillance involving the collection, sorting and aggregation of data sets to identify, track, monitor, predict and constrain personal behaviour (Clarke, 1988; Raley 2013; Kitchin, 2016). Such surveillance is possible thanks to vast quantities of available data and contemporary analytical techniques. With the extra data it collects, IoT can play a key role in bolstering dataveillance.

[51] Some writers include in the concept of surveillance intentional or unintentional *subveillance* on oneself by others, using "smart" technologies. Please see Appendix E for more information on this topic.

Dataveillance involves *real-time* data harvesting and storage of vast quantities of bulk digital data from different sources. Harvested data may be generated by personal digital devices (smart phones, computers, wearable computers, credit cards, RFID tags, etc.), lifelogging,[52] digital social networks and other connected apps, as well as interactions with different sensors throughout the city. Collected data is a resource that can be subsequently enhanced through aggregation with other data. According to Rouvray and Berns (2013), this kind of constant data collection other than for predictive purposes and without any specific purpose is unprecedented in the history of profiling (Rouvroy and Berns, 2013). Analysis, primarily of correlations between data, follows, with digital duplicates (Haggerty and Ericson, 2006; Rouvroy and Berns, 2010) generated, along with various predictions of personal behaviour. This process clearly demonstrates that the larger data quantities generated by urban IoT would imply more effective and precise analyses for use in monitoring individuals.

In addition to all of the previously mentioned issues of self-censorship, disempowerment and suppression of minority viewpoints, dataveillance, and in particular, preemptive prediction,[53] pose challenges to the presumption of innocence rule. Lack of transparency with respect to the data, accompanied by algorithmic reasoning, as well as decision-making based on the expectation of bad behaviour, may contravene the principle that everyone is presumed innocent unless convicted. We must now be suspicious in advance, contrary to the doctrine that that we should "first, trust the word of others, then doubt if there are strong reasons for doing so" (Ricœur, 2000), in line with the concept of social habitus and rules of prudence. This stance undermines our sense of community and the social bond. Omnipresent, constantly accessible data becomes a "proof" of anything and may replace all testimony, or even discussion, dealing a heavy blow to social harmony and increasing "social anxiety."

8.1.2 Potential Threats in Data Analysis

Three threats to freedom have been identified at this step:

- Prescriptive analyses, which guide personal choices.
- Predictive analyses, which determine individual access to opportunities.
- Profiling, which inhibits people's natural ability to transform themselves.

[52] Lifelogging is the accumulation of quantitative personal data concerning different aspects of a person's life (health, relationships, sports performance, etc.). Please see Appendix E for more information on this topic.

[53] Please refer to the next section on forecast analysis for additional information on preemptive prediction.

Section 5.1.2, above, identifies possible threats associated with data analyses used for forensic profiling.

Predictive Analyses that Guide Personal Choices

Kerr and Earle (2013) proposed a general typology of anticipatory algorithms that predict human behaviour. Two of the three types may be relevant to the Urban IoT project.[54] They are:

- Preferential prediction.
- Preemptive prediction.

Preferential prediction concerns opportunities and choices that people should have. It employs machine-learning algorithms to predict which information and products are likely to interest consumers. Based on their digital profiles and activity histories, people are offered choices that presumably "match these profiles." Clearly, the most striking example from the private sector is Amazon's 2013 recommendation technology patent filing: based on digital profiles, the technology makes it possible to ship merchandise to customers before they have even thought of buying it (Bensinger, 2014). These strategies are certainly aimed at making information and product searches more efficient for people, while at the same time they serve to channel and limit personal choices and, generally, to offer more or less the same kinds of content that people previously selected (Taylor, 2014). The question arises: how much autonomy do people have when choices about their own lives are constantly inferred by others?

Predictive Analyses Determining Personal Access to Opportunities

Preemptive or prescriptive prediction is intended to facilitate decisions on providing a person (or group) with access to services or opportunities. If algorithm-based predictive analyses and profiles can be consulted by third parties or are subject to automated decision-making, they can have a major impact on finding work (depending on employability score), getting credit (depending on credit rating), obtaining health or car insurance (depending on risk rating), being admitted to a school, etc. People may not be able to receive certain services, based on their digital duplicates.[55] Such techniques, of course, also apply to profiling for public safety purposes.

[54] The third type is consequential prediction, which seeks to predict the consequences of people's actions, so that they can be encouraged to follow rules "to improve" their conduct. Please see Appendix E for more information on this topic.

[55] Observers note, however, that the "knowledge" produced by algorithms is inferred through correlations (and not the other way around), depending on selected criteria. This process can be perceived as being more objective because it is machine based, but it remains subject to incorrect interpretation. It could even confuse corelationships with causality—accompanied by a severe impact when legal decisions are based on such data.

Box 9: Inability to Dispute Decisions Based on Preemptive/Prescriptive Prediction

Preemptive or prescriptive prediction also raises the issue of people's ability to dispute algorithm-based decisions about them. People usually have no way of determining the paths taken by collected data or the information generated by algorithms. Several observers describe a loss of control due to the fact people do not know when or how their profiles are used (Kitchin, 2016). The relatively unintelligible nature (even for programmers) of algorithmic reasoning makes it far more difficult to appeal a decision (Kerr and Earle, 2013). Giving an account of yourself or your actions when faced with algorithmic decisions and assumptions is a fundamental challenge. The right to explain yourself, particularly in a legal situation, must not be eclipsed by correlational statistics used as "objective" evidence.

The importance of potential remedies has also been discussed in detail in the Section 4 (Ethical Issue: Privacy) and Section 5 (Ethical Issue: Social Inclusion).

Profiling Inhibits People's Natural Ability to Transform Themselves

Profiles built around a plurality of data values obtained from within a person's environment creates a lasting portrait of that person.[56] As Rouvroy wrote, though, one key to personal empowerment is "the opportunity to see your life not as a confirmation or repetition of your data tracks, but as a chance to change direction, explore new lifestyles and ways of living—in short, to do what others, and even you, do not expect" (Rouvroy, 2008). With large-scale deployment of algorithmic profiling, it will become increasingly difficult for people to start over. As Mannermaa wrote, the ubiquitous surveillance society never forgets (Mannermaa, 2007, 112).

[56] A kind of "total digital memory."

8.2 Potential Solutions

This section outlines a few additional tentative solutions to ethical issues of personal freedom that were not previously discussed in this report.

8.2.1 Respecting Privacy Rights

Section 4, above, discussed many recommendations on this topic. The literature on the concept of freedom particularly emphasizes the following points:

- Minimizing collected data by limiting collection to data corresponding with publicly stated goals.
- Telling the public how the data collected will be used.
- Adopting the policy of deleting unused data.
- Adopting a policy on data reuse–other than in exceptional cases, data should not be used by any parties that have not been described and stated in advance (Abiteboul and Froidevaux, 2016).

Several of these points—especially those concerning minimizing data collection and restricting data reuse—run counter to the IoT project's goals of collecting big data to encourage extensive reuse. City agencies must learn how to deal with such conflicts over coming months and years.

8.2.2 Building a Regulatory Framework Around Certain Kinds of Algorithmic Predictions and Deciding Which Should Be Banned

The section on social inclusion (5.2.7), above, discusses this option, which also applies to the issue of freedom.

8.2.3 Developing Policies on the Right to Comment on and Contest Data

This means formalizing the public's right to dispute algorithmic decisions that concern them personally. Rouvroy recommended that, in addition to this requirement, the burden of proof be reversed, making a person or institution using algorithms responsible for demonstrating, for example, that there was no discrimination. These means offering a rationale for algorithmic decisions that ostensibly affect a particular individual (Rouvroy, 2016, 49). This approach enables each of the parties to communicate, speak freely and give their reasons. Such a requirement to provide explanations does not relieve institutions using algorithms of their responsibilities. The section on privacy issues (4.5.5) also discusses access to redress mechanisms as an option (4.5.5).

8.2.4 Developing Policies on the Right to be Disconnected

This right serves to reassure people that there is no digital profile on them or that their personal data is only partial. “Disconnected” also means “non-digital” and lets people go on with their lives outside the digital realm. Paying tuition online, voting online and making doctor’s appointments have become so predominant it is sometime difficult to do something without using a digital platform. Initiatives aimed at maintaining face-to-face services are very useful in helping people go digital—or not.

8.2.5 Developing Policies on a Right to be Forgotten

The right to be forgotten is a recent legal principle that does not apply in Canada.[57] It is generally defined as “the right to remove or inhibit access to accurate, inaccurate and obsolete online information—whether accurate, inaccurate or obsolete—about a person’s past, so they can be removed the collective memory and forgotten” (Lecomte, 2017). In current jurisdictions, such as Europe in particular, it is the right to delete and correct personal—and generally publicly accessible—digital data. Applying a right to be forgotten to big data—a technology falling into the grey space between private and public life—is a real but important challenge, given the existing legal vacuum on this topic.

Box 10: Right to Erase Data

Article 17 of the European Regulation of 27 April 2016 provides the right to the erasure of personal data. Article 65 adds that “A data subject should have the right to have personal data concerning him or her rectified and a **‘right to be forgotten’** . . . In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her . . .” (European Parliament, 2016).

[57] However, the Office of the Privacy Commissioner of Canada has been examining the right to be forgotten since 2016 (Lacombe, 2017).

8.3 Is Algorithmic Bias a Necessary Evil in Ensuring Public Safety?

On November 25, 2016, Piotr Smolar published an interesting article in *Le Monde entitled*: "Secret Algorithms for Israeli Surveillance in Jordan." We mention this here because it illustrates the complex nature of applying potentially discriminating algorithms to public security purposes.

Piotr Smolar explained that the Israel Defence Forces (IDF) use profiling apps to detect suspect profiles on social networks. "*This prevented hundreds of attacks, even if we cannot be certain that every person identified would have perpetrated one imminently"* (Smolar, 2016). Machine-learning algorithms are accordingly designed to forecast when someone will go from word to deed, permitting his or her apprehension prior to the crime, even when there is no objective evidence to suggest a terrorist attack was about to occur. Guillaume Champeau (2016), another journalist who wrote on a similar topic, said:

> *"According to an Israeli official questioned by a press agency, they constantly draw up suspect profiles, not only using metadata on a person's communications and habits, but social networking exchanges, of course."* (Champeau, 2016)

Questions of privacy rights and freedom hold little sway in this security scheme. Will making exceptional surveillance measures the new normal give governments powers that, in democracies, fall under the justice system?

9 Transforming Governance Modes

The literature on social issues associated with the smart city and IoT suggests that IoT deployment will cause basic changes in governance.

While not exactly "ethical issues," such factors remain important in a city government's day-to-day activities and interactions with residents. Such changes should accordingly be considered in any assessment of an IoT project's social acceptability.

9.1 Internet of Things: From Driver of to Factor in Change

The digital era is here and it is high time to focus on governance! According to the Governance Working Group of the International Institute of Administrative Sciences (1996), governance is a process that enables social forces to exert power and authority, define policies and make or influence decisions on public life, as well as social and economic development. Governance implies interaction between formal institutions and civil society.

The document *Infrastructures et villes intelligentes* by the Commission de la science et la technique au service du développement (Conseil Économique et Social, 2016) does not describe the smart city as a resource for executing an urban plan, but as a means of renovating municipal governance. Studies on digital governance reveal changes in governance itself. IoT, in other words, is not merely a technical innovation to be considered for adoption by Montréal, but the source of new governance issues with which they city must contend. We shall discuss this in greater depth, below.

9.1.1 Factors of Transformation in Municipal Governance

All of the identified factors pertain to the technical orientation typical of IoT-based governance, where technology plays a dominant role in governance and decision-making. This technological focus entails a depolitization of the concerns a smart city is expected to address. The vast urban IoT project is presented primarily as a technological, apolitical effort that makes "good sense." This approach minimizes debates over priorities and proposed solutions and, in so doing, reduces the chances of social opposition (Douay and Henriot, 2016).

The key factors involved in transforming urban governance are all present throughout the data analysis phase. They are:

- Decisions aimed at optimization, not social optimums or basic causes.
- Dilution or loss of decision-making authority.
- Deterministic representations of the world.
- Fewer options.

Decisions Aimed at Optimization, Not Social Optimums or Basic Causes

A key function of machine-learning algorithms is to drive optimization. Once again, though, this ideal must be defined and, if necessary, rejected in favour of a less efficient or cost-effective but "smarter" solution that actually solves the social problem in question and not just the particular calculation the algorithm is designed to make. Achieving such optimization is a technical matter. It is important to know how to benefit from this optimization, but this is not the same as a social optimum, which results from compromise. Algorithm optimization seeks to achieve multiple (technologically, economic, political, ecological, etc.) optimums, which, when grouped together, can be weighed, discussed and expressed. Strictly speaking, societies do not "function" (G. Canguilhem).

As Kitchin noted: "On their own, technical solutions cannot address basic problems because they do not deal with their root causes. These solutions should, instead, make it easier to deal with manifestations of such problems" (Kitchin, 2014b).

Dilution or Loss of Decision-Making Authority

Two points on this topic bear mention. First, algorithms generate output expressed as decisions, such as categories and recommendations. Potential human-machine interactions in decision-making fall within a continuum ranging from mere consultation to total delegation of responsibility to these analytical systems. We are witnessing a dilution or loss of decision-making accountability where algorithm optimization takes the form of decisions and actions, without people being able to explain the reasons for results, even after the fact.

Deterministic View of the World

In seeking predictability of human and non-human phenomena, people increasingly turn to "stable" correlations based on machine learning and algorithm analysis. The mass data used in different formats, from different sources and in astronomical quantities, is encouraging humans to reduce situations to deterministic models (Floridi, 2012). Doing so creates a situation in which structures are locked into the past. Predictability transforms symbolic representations of the present into a new category, known as "Permanence." Believing that the present is better than the unknown is called "conservatism." However, we know that life is characterized by its many new and totally unpredictable—but fascinating—changes of trajectory (Heisenberg, 1990).

Fewer options

In his study of the smart city, Kitchin noted that its form of governance presupposes that all of its dimensions can be measured, monitored and handled in the same manner as technical issues. He emphasized that this approach can shrink the range of options and analyses considered, in line with the data available. The analytic "focus" is confined to raw data that can be transformed into easily manipulated data (Kitchin, 2014b).

9.2 Potential Solutions

9.2.1 Municipal Assumption of Full Accountability for Project

Decisions based on algorithm analysis should help identify key moments and factors in municipal decision-making, so the city can assume full accountability for the technological system deployed. Such decision-making assumes that employees are trained in-house to discuss delegations to technology, to avoid the bureaucratic trap of replacing "it's not me, it's the system," with "it's not me, it's the algorithm." If the government primarily assumes the role of delegating, without supervising, its authority will be diminished and it will be unable to account for its own actions.

This is why we should envision our relationships with technology in terms of a technological culture that enables us to think of technological devices as part of society—and not merely instruments that automatically take over our decision-making. A healthy government assumes its full role as primary decision-maker and administrator, while giving civil society full reign to criticize and reclaim decisions that have been made and preferred management techniques (folksonomy, collective mapping, etc.).

9.2.2 Promoting Public Participation in the Project

We must begin by considering how residents can be part of this project, while also focusing on the development of infrastructure and smart services. Of course, it would be necessary to educate, train and prepare these stakeholders properly for working with machine-learning algorithms. The smart city will also—and perhaps primarily—involve members of the public unable to choose between good and bad uses of algorithms. This means that the biggest public investments should be in education—even more than in infrastructure and networks.

In other words, in addition to ensuring optimal management of workflows and smart infrastructure, the most urgent issue is determining the role the public is expected to play as stakeholders and subjects of a project that will grow—rather than shrink—their *autonomy* (as defined by Malherbe, 2000). Technological systems must be built around social initiatives. Otherwise, infrastructure spending may amount to little more than conspicuous consumption or short-term urban window dressing for investors.

9.3 DISCUSSION: The Proper Roles for Automation and Algorithms in Society

It is odd to instinctively label technological systems as “smart” when they seem to perform activities or functions *automatically* that we were previously accustomed to doing on our own. However, the term *automated* typically infers low intelligence or little imagination. In fact, the term *automation* is not suited for designing and optimizing public policies and city management.

The automation paradigm is, in fact, so outmoded, that machine-learned output cannot always be analyzed by the engineers who designed it. It has become increasingly difficult for engineers to trace the algorithmic steps leading to a result. We can no longer require that these algorithms be both automated and innovative or autonomous. In terms of policy, the issue is what we ask our machines to do.

Automation is actually a very low bar, which says more about our lack of technical knowledge (being able to run a machine properly and contribute actively to its redesign) than the technological system’s intrinsic quality or performance (G. Simondon; G. Canguilhem). If we really want to live in smarter cities, with algorithmic systems embedded within the urban fabric, such systems must be better integrated with our values and ethics. This means thinking of algorithms as an integral part of the governance and management processes and as social actors offering certain benefits—and drawbacks (H. Collins). Viewing algorithms in terms of their integration within the social fabric means employing them appropriately, based on our knowledge of a situation, rather than falling into the trap of universal automation, based on a conviction that automated institutions and activities are better, more efficient and more cost effective.

10 Social Acceptability and IoT

10.1 Definition of Social Acceptability

Québec's French-speaking sociologists[58] who are studying, using and developing the concept of social acceptability in Canada share two points of agreement: (1) They recognize a multi-stakeholder consensus that this concept is useful in identifying and understanding the wide range of positions on an urban development project. (2) They believe the concept is ambiguous, unclear and even dubious. This is because, despite the shortcomings of social acceptability as an analytical category, it can be considered a critical grouping, which each stakeholder injects with meaning, depending on that individual's relationship to the project. The meanings assigned to this concept over the course of a project become quality indexes of the deliberative/consultative mechanisms employed. Consequently, the concept of social acceptability seems to promote the creation of a multi-stakeholder, multi-level governance system in the case of Montréal's IoT project.

With this in mind, we must assess the relevance of the various definitions offered. This work has been done in part by Pierre Batelier (2015). Some of the most-cited definitions in the Québec literature appear in Appendix G. As an analytical starting point, however, we shall adopt the definition of social acceptability proposed by Corinne Gendron (2014), which has generated some consensus and seems useful in guiding our discussion:

> "The public sentiment that a plan or decision resulting from collective wisdom is better than the known alternatives, including the status quo*."* (Gendron, 2014, p. 124).

This definition, adapted from that of Brunson, et al. (1996), views social acceptability as the result of a collective decision, involving informed choices, with a particularly good understanding of potential opportunities and benefits, as well as risks. It is also apparent that this collective judgment is based on community or group values, which are neither uniform in every situation or set in stone. This is because opinions can change over time, in accordance with events and the public's growing interest in or polarization around a topic that generally triggers opposition, and ultimately, increased quantities of accessible information.

[58] Marie Josée Fortin, Corinne Gendron and Pierre Batelier, mentioning only the best-known members of this group.

10.2 Social Acceptability of the Urban IoT Project

10.2.1 Social Acceptability of the Smart City and Social Factors in the Smart City

We have, to date, only found one bibliographic reference, taken from an academic journal, entitled "Smart City concepts: from perception to acceptability" (Schelings and Elsen, 2017). Other writers mentioned below discuss the smart city's social dimension, but not its social acceptability. This initial reference is drawn from the work of Belgian researchers Schelings and Elsen at the Université de Liège, who developed a questionnaire used at three separate smart city events in Belgium to assess the smart city's social acceptability.

Their questionnaire was completed by 125 participants in these events (attended by a total 625 people), who were members of the public or professional stakeholders in the smart city project (government officials and service providers). All these people can be considered not just interested in, but knowledgeable about the smart city (Schelings and Elsen, 2017), due to their presence at these events. The questionnaire covered different fictional smart city scenarios and did not pertain to any particular city.

This study, which is worth reading, demonstrates that the major concern of those surveyed was the "personal," far more than the economic or environmental, aspect. The top concern was personal privacy. Public participation in governance of the smart city also appears as a theme that is important—but far less so than personal data protection.

> "*'Private data' nevertheless emerge as one key aspect participants would be reluctant to share, which underlines the delicate balance one has to reach between collecting large amount of data (essential to nurture Smart City initiatives) and insuring end-users' privacy and anonymity*" (Schelings and Elsen, 2017, p. 3).

It is worth noting that this initial study on perceptions and social acceptability of the smart city was conducted using a psychosocial approach among a sample group. For this reason, the study benefits from considering the concerns of many people and not just one writer. Kornberger, et al. (2017), applying a similar methodological approach, predicted a "shock" when the bureaucracy is confronted with a new open data policy in rolling out a smart city project for Vienna.

The authors expected a clash of values within city government, which had little experience in or talent for sharing its data and discussing decisions with the populace. In the case under study, the researchers found that official concerns focused on two areas: (1) Officials' perceptions of their accountability in an open-data system, where data is available to everyone for a wide variety of uses outside their control. (2) Transparency (because open data raises questions about how the released data is selected and implications for the city).[59]

[59] In the case of Montréal, some of these questions have already been discussed and examined in depth following implementation of Montréal's Open Data Policy and Directive on Data Governance. The fact that data collected by the city is owned by the city serves as a solid foundation for considering the foregoing topics.

Rather than presenting the results of a sociological or psychological study, Monfaredzadeh and Krueger's article (2015), *Investigating Social Factors of Sustainability in a Smart City*, underscores the importance of taking the social factor into account as a prerequisite for a smart city project's success.

> *"Smart cities initiatives allow members of the city to participate in the governance and management of the city and become active users. An individual must be able to connect in order to achieve enhancement of social and cultural capital as well as achieve mass economic gains in productivity. If they are key players they may have the opportunity to engage with the initiatives to the extent that they can influence the effort to be a success or a failure"* (Monfaredzadeh and Krueger, 2015, p. 1113).

This kind of work is fully aligned with that of Lewis Mumford (1937) who, even in his day, argued that urban planning suffered from a lack of surveys on the city's social functions. Chris Landford (2011) tackled this problem by proposing a matrix of variables to consider in assessing the social sustainability of an urban environment. Landford's work does not, however, consider digital infrastructure.

The academic literature now favours a *shared city* approach to bolstering public participation. This school is part of a global trend toward public participation, corresponding with a hypermodernistic version of public-spiritedness—a 21st century style of public engagement promising gains in efficiency and transparency, while nurturing hopes of social change.

10.2.2 Use-Phase Studies

If we slightly expand our field of research, we see that engineering use-phase studies (published since the 1980s) also delve into the social acceptability of technologies and infrastructures, focusing on the use of the object under study. A use-phase study employs timelines showing how users do (or do not) adopt a product, service or infrastructure (Terrade, et al., 2009). The use phase is often broken down into three sequences: utility, usability and social acceptability.

"Utility" refers to correspondence between functions supported by the system and user-assigned goals. Put another way, utility is the partial or total conformity of the system's features with current or future user goals. Usability is the ease with which a system's features can be used and consists of five aspects:

1. Ease of learning.
2. Potential performance.
3. Recollection of features.
4. Error prevention.
5. Satisfaction.

In other words, "utility" is the correspondence between what the product, service or infrastructure is likely to do and what the user wants it to do, while "usability" refers to its ease of use (Tricot, et al., 2003). Sociology, science and marketing have empirically demonstrated that an innovation can be very useful and usable without it being adopted by individuals or society.

Studies have also delved into the question of an object's social acceptability, but with far less detail or structure. Such research considers a use's sociocultural context, which could undermine the system's predicted acceptability, based on its utility and usability, in cases of certain innovations and under certain circumstances.

While many use-phase studies examine social acceptability, they do so from the perspective of individuals and their interactions as a user with a product or an infrastructure. This approach is inconsistent with the prevailing definition of social acceptability, which emphasizes collective, not individual, judgment.

Box 11: Acceptability Evaluated at Three Points in Time

Use can be considered at three points in time.

- Before use: Evaluation before a person has used the product/infrastructure. Acceptability reflects the user's subjective impression, in consideration of the product's or infrastructure's perceived: (1) utility, (2) perceived usability, (3) presumed social influences and deployment conditions.
- After use: Evaluation in an experimental framework, once an individual has had a chance to use the product/infrastructure at least once. The same three factors are considered, with emphasis on the first two.
- Following integration into the daily life: Evaluation of the service's or infrastructure's actual adoption, once it is made available to the users for inclusion in their daily routines. The same three factors are considered, with emphasis on the first two (Tricot, et al., 2003).

10.2.3 Findings on Social Acceptability and the Urban IoT project

The literature review shows that the issue of social acceptability of urban IoT projects–whether from a personal (in use-phase studies) or collective (in sociological studies) perspective–has received less attention than ethical issues.

It is impossible at this stage to identify the smart city's "social acceptability" issues with confidence, either in general or with respect to Montréal. However, this report lists a variety of issues and concerns that could entail public opposition to an urban IoT project and constitute impediments to the project's social acceptability.

Sections 4 to 9 of the report describe ethical issues pertaining to privacy, social inclusion, separation of the government and business spheres, transparency, reliability and freedom, as well as those concerning changes in governance modes that could trigger social opposition. The literature also refers to other concerns, which cannot be classified as ethical issues, because they are not clearly based on basic social principles (although this point is open to discussion), but could be the subject of social opposition. Then there are concerns about certain IoT system components, in light of recent events in Québec—such as worries about the proliferation of Wi-Fi transmissions in public areas, opposition in 2011 to Hydro-Québec's smart meters, with many citizens speaking out against having more Wi-Fi waves passing through their homes—which underscored sensitivity to this topic. However, the literature review did not identify any issues of this kind with respect to IoT.

Figure 5, below, illustrates the ethical issues, along with most of these concerns—or in other words, the various issues with the potential to harm the project's social acceptability. Section 10.2.4, below, describes the identified concerns in detail.

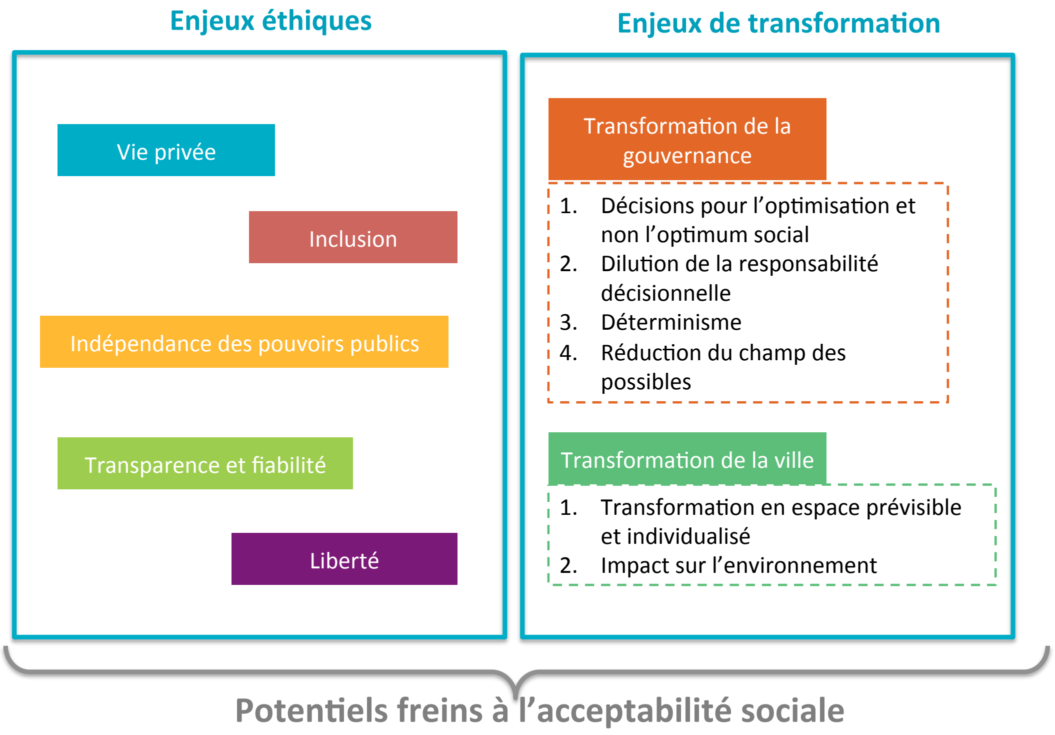

Enjeux éthiques
Vie privée
Inclusion
Indépendance des pouvoirs publics
Transparence et fiabilité
Liberté
Enjeux de transformation
Transformation de la gouvernance
1. Décisions pour l'optimisation et non l'optimum social
2. Dilution de la responsabilité décisionnelle
3. Déterminisme
4. Réduction du champ des possibles
Transformation de la ville
1. Transformation en espace prévisible et individualisé
2. Impact sur l'environnement
Potentiels freins à l'acceptabilité sociale

Figure 5: Potential Impediments to Social Acceptability

The following box describes the only poll to date on how Quebeckers feel about IoT. While the topic is covered generally (and not specific to one city), it does highlight trends worth mentioning.

Box 12: Quebeckers and IoT

According to CIRANO, Quebeckers believe that the benefits of using the Internet of Things outweigh the risks. Seventy-three percent of Quebeckers support using things connected to the Internet and sharing the information, while 45% believe that such use is somewhat or highly beneficial to Québec. On the other hand, 20% of Quebeckers have little or no confidence in their government's management of how connected things are used. This means a bit less than one third of all Quebeckers feel there is a risk in using such technology. Between 40 and 50% of Quebeckers would be prepared to share data on their health, housing, travel and driving behaviour (CIRANO, 2017).

10.2.4 Identified Concerns

Identified concerns that do not constitute ethical issues or pertain to changes in governance modes are described below. Such concerns are often those of the writers and not based on results of a sociological or psychosocial study of current or future smart city residents.

Table 1: Identified Concerns

Concerns	Argument
Turning the city into a "predictable space"	Many writers caution against over-planning urban trends, arguing that this perspective is changing the city's role as a lived-in space and diminishing quality of life. Algorithms and the processing of underlying data reflect a unique vision of the city, driven by these systems themselves. Technological architecture is similar to urban aboveground architecture, where streets and buildings form spaces and venues—or eliminate such spaces (Kitchin, 2014). Recommender systems reduce stimulation levels, exploration of new routes, chance encounters between residents, etc. The constant search for efficiency thus appears as an obstacle to city life—in the sense of undirected activity and wandering around with no specific purpose (Sassen, 2011).[60]
Individualization of the city	Personalized access to certain services or information (such as advertising that targets specific tastes, travel tips from downloaded apps based on recorded preferences, etc.), gives rise to in unique personal urban experiences. In the same way, social network algorithms and search engines generate spirals of content that continuously shrink to more succinct and selective content. Widespread use of filtering apps leads to different experiences in and a different understanding of the city based on this vortex model. Developing "à la carte city" mechanisms, where residents are described as users or clients of services provided by the city, gives them access to a range of free and paid services (Baraud-Serfaty, 2011). The Bordeaux 3.0 project is one example of this phenomenon.

[60] One practical example is an app that points users to any of Vienna's public toilets. What is the risk that tourists discover fewer sites by strolling aimlessly, because the app has shown them the shortest path to a restroom?

Turning the public into a consumer of services	Some writers also explain that the role of residents in smart city projects is, similarly, a vector of depolitization and dehumanization. According to smart city rhetoric, the exercise of civic rights is often seen primarily from an economic perspective, with the creation of services and applications sold to people who are perceived only as customers. Participation in urban sociopolitical life consequently takes shape primarily in terms of creating products for sale, more than with respect to community action. Residents accordingly assume the role of consumers of services offered by city government, or by other individuals or business, rather than political players. This dynamic corresponds with an "uberization" of the economy that many writers have lambasted. This widely publicized concept refers to the process of commercializing services and ties between members of the public (Morozov, 2015).
Fear that cities will become homogeneous and "standardized"	Many writers have mentioned the homogenization that afflicts cities in the process of becoming "smart." This is because the strengths of cities lie less in their "IQ score" or international clout, but in their distinctive features, the ways they stand out and their areas of specialization (Sassen, 2011). Smart city projects are often similarly designed throughout the world, because they rely on technological resources that are alike from one city to the next (Poty, 2014). From this viewpoint, the smart city is a commercial product, with the very idea developed by service providers (Townsend, 2013). Consequently, there is a concern that "smart city systems" supplied by such providers will be reduced to generic products that fail to treat each city as a separate entity, with its own characteristics (sociocultural, economic, geographic and historic qualities) (Kitchin, 2014). It is these very factors, however, which reveal each city's real intelligence potential. This lack of differentiation results from such factors as how the smart city project is understood. Categories developed to describe smart governments and international classifications of a city's smartness fail to consider these distinctions and produce unequivocal visions (Poty, 2014). Nonetheless, what works in one city may not in another (Sassen, 2011).
The smart city's environmental and energy cost	Smart infrastructure often permits optimizing the use of various resources, saving energy and boosting efficiency. Digitalizing numerous services also makes it possible to cut production and resource consumption (paper and stationery, office supplies, etc.). Relocating municipal jobs cuts costs and consumption (employee travel, office energy consumption, etc.) (Baraud-Serfaty, 2015). These savings of energy and resources are often employed to trumpet the merits of a sustainable smart city project. However, many writers have cautioned against mere shifts in consumption. Such shifts occur geographically within the city and its suburbs with respect to types of consumption produced by smart city tools. The propagation of servers, smart phones, computers and other connected objects, as well as the resources deployed for their maintenance (coolers, uninterruptible power supplies, generators, etc.), consume vast amounts of power (Viitanen and Kingston, 2013). Finally, this shift is occurring worldwide with an impact on social and environmental justice.

11 Conclusion: The Smart City's Promise

This report provides an overview of academic studies on issues of ethical and social acceptability associated with deployment of an Internet of Things in urban infrastructure. While studies on ethical issues pertaining to the Internet of Things are promising, we are at this point merely considering researcher hypotheses on the smart city's social acceptability. Much work remains!

We have given equal weight to all the arguments contained in this report, since it was impossible to take into account all of the thousands of articles written on this topic. At this stage of the work, we do not wish to weigh arguments, solutions or ideas. That exercise is essential, however, and we will do so in Phase 2 of this project, working in close conjunction with Montréal's team. This approach is inspired by our commitment to maintain the impartiality expected of a summary report.

Our mission, as you know, is of the greatest importance. We have a chance to *determine how well a promise is received.*

A promise is speech. What is offered by the promise is words. The value of such words are intrinsic to themselves and not to the meaning of the promise. In other words, it is the deed that counts. It is the deed that gives time! It gives time, because from the deed, the world becomes the World for the first time.

The promise creates a potential, rather than a future. It falls within the range of the possible, but also generates expectations. For Jacques Derrida, a promise has a three-part *already-not-yet* structure.

> "*Of the past, erased, singular event (an origin, a trauma, an appointment), there only remains an inaccessible, lost trace, which gives rise to a still masked truth, supposedly known, but concealed and not yet revealed. The promise, which is built around this expectation, supplements and exceeds it. We always promise too much. This 'too much' is the essence of the promise, making it confusing and disturbing*" (Derrida, 2009).

Jacques Derrida wrote that the promise constitutes excess! An "excess" that always complicates the task of institutions making it. We shall return to this topic, as we wish to examine the link between ethics and promises, before proceeding further.

> *"Perhaps more than in other types of verbal performance utterance, the promise commits its maker to a future involving its identity and responsibility with respect to third parties and society. As wary as people are about promises, they remain a cornerstone of society. They are an appropriate—yet disturbing—form of speech. The promise embodies the force needed to drive all social life and is beyond the grasp of institutions" (Grieu, É. and Thomasset, 2005, p. 75).*

The promise, in fact, is a vehicle of the ethics it nurtures: (i) perseverance, (ii) duty to act and (iii) responsibility (Nachi, 2003). In addition to these core roles, Alain Boyer adds that the promise creates the obligation of *something promised, something owed*. Indeed, the promise lets us see hints in the present of newly emerging life.

As previously noted, all institutions make promises. We shall now discuss how difficult it is to accept promises from institutions, because of their social acceptability. Past and contemporary disasters have inoculated us against a belief in promises. This sentiment is not only reflected by leading schools of thought, but the suspicions about any proposal that would influence the course of events. Such public skepticism of promises is magnified by our awareness of the fragility of life. Those who believe sweeping promises risk being perceived as naive or true believers.

Making a promise means asking someone to trust that something will come true in the future. It is only over time that we can determine if the promise was kept. A promise is unique in that the mere idea of an excuse is inapplicable. That is why we must now carefully consider the different options we have described to address the ethical issues and social acceptability of the Internet of Things in providing our best support in making the Ville de Montréal an icon of the smart city's promise.

12 Bibliography

Abiteboul, S. and Froidevaux, C. (2016), “Autour de l’informatique : algorithmes et la disparition du sujet. Interview with A. Rouvroy,” *The Conversation*. Viewed at: http://theconversation.com/autour-de-linformatique-les-algorithms-et-la-disparition-du-sujet-53515. Viewed February 20, 2018.

Amossy, R. (1989), “La notion de stereotype in the réflexion contemporaine,” *Mutations d'images.* 73: pp. 29-46.

Ananny, M. and K. Crawford (2016), “Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability,” *New Media & Society*: https://doi.org/10.1177/1461444816676645

Angelidou, M. (2014), “Smart city policies: A spatial approach,” *Cities* 41, Supplement 1: S3-S11.

Baraud-Serfaty, I. (2011), “La nouvelle privatisation des villes,” *Esprit* 3 (March/April): 149-167.

Barocas, S. and H. Nissenbaum (2014), “Big Data's End Run around Anonymity and Consent,” *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. J. S. Lane, Victoria. Bender, Stefan. Nissenbaum, Helen, eds. New York, NY, Cambridge University Press**:** pp. 45-75.

Batini, C., Cappiello, C., Francalanci, C., and Maurino, A. (2009), “Methodologies for data quality assessment and improvement,” *ACM Computing Surveys (CSUR)* 41(3).

Battelier, P. (2015), “Acceptabilité sociale, cartographie d'une notion et de ses usages,”*Cahier de research*, UQAM: Les publications du Centr'ERE.

Bensinger, G. (2014), “Amazon Wants to Ship Your Package Before You Buy It,” *The Wall Street Journal*. Jan. 17, 2014.

Berthier, T. and O. Kempf (2016), “Vers une géopolitique de la donnée,” *Réalités industrielles.* August 2016.

Birman, J. (2011), “Je suis vu, donc je suis: la visibilité en question,” *Les tyrannies de la visibilité*. Aubert, N. and Haroche, C., eds. Toulouse, Ères coll,” *Sociologie clinique***,** pp. 39-52.

Brender, N. (2012), “Étude du dilemme urbain : urbanisation, pauvreté et violence,” C. Summary document. Written by Natalie Brender, based on the study by Robert Muggah, CRDI.

Breux, S. and J. Diaz (2017), “La ville intelligente : origine, définitions, forces et limites d'une expression polysémique,” U.U.d. recherché, Montréal, Institut national de la recherche scientifique.

Brunson, M., et al. (1996), *Defining social acceptability in ecosystem management: a workshop proceedings. Gen. Tech. Rep. PNW-GTR-369.*, Portland, OR.

Bunker, E. (2016), *Aucune bête aussi féroce*, Payot and Rivages.

Carcassone, G. (2001), “Le trouble de la transparence,” *Pouvoirs* 97: 17-23.

Cardon, D. (2015), *A quoi rêvent algorithms - Nos vies à l'heure des big data*. Paris, Le Seuil.

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

Canguilhem, G. (2015) “Le normal et le pathologique,” Paris, Presses Universitaires de France, *Quadrige*, 2015, 12th edition.

Champeau, G. (2016), “Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël.” *Elnet*.

CIRANO (2017), *Baromètre des perceptions des québécois*, *Presse internationale Polytechnique*.
Available at: https://barometre.cirano.qc.ca/pdf/issues_sante.pdf

Citron, D. (2010), “Technological Due Process.” *Washington University Law Review* **85**: 1249-1256.

Clarke, R. (1998), “Information Technology and Dataveillance,” *Communications of the ACM* **31**(5): 198-512.

Collins, H. (2003), *Enterprise Knowledge Portals*, AMACOM.

Commission de l’éthique en science et technologies Québec (2017), “L’éthique et la morale, de quoi on parle ?” Retrieved July 22, 2017, from http://www.ethique.gouv.qc.ca/fr/ethique/quest-ce-que-lethique/lethique-et-la-morale-de-quoi-on-parle.html.

Commission de la science and la technique au service du development. (2016), *Infrastructures et villes intelligentes,* UN Economic and Social Council, United Nations.

Crawford K. and Schultz, J. (2014), “Big data and due process: toward a framework to redress predictive privacy harms,” *Boston College Law Review* 55(93): 93-130.

D'Elbée, P. (2015), “L'exigence de l'humain face à la technique,” *Raisonnance. Cahier de réflexion des maires francophones* (6): 22-25.

Delain, P. (2017), *Les mots de Jacques Derrida,* Ed: Guilgal, 2004-2017. Page created August 25, 2005.

Delain, P. (2017), *La promesse. 1. Archi-promesse,* Ed.: Guilgal, 2004-2017, Page created July 5, 2009.

Deleury, E. (2016), "Ville intelligente : le numérique et l'éthique doivent aller de pair," *Huffington Post,* 2016-02-24.

Desmond, M. (2012), "Eviction and the Reproduction of Urban Poverty," *AJS* 118(1): pp. 88–133.

Doran, M.-A. (2014), "Démystifier les villes et communautés intelligentes," *Le Sablier* 21(1): pp. 20-29.

Douay, N. and C. Henriot (2016), "La Chine à l'heure des villes intelligentes," *L'Information géographique* 3(80): pp. 89-102.

Dusek, V. (2006), *Philosophy of Technology: An Introduction*. Oxford, Blackwell Publishing.

Erlingsson, U. e. P., Vasyl and Korolova, Aleksandra (2014), "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response," *Proceeding of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. Scottsdale, Arizona.

Federal Trade Commission (2015), *Internet of things: Privacy and security in a connected world***,** p. 71.

Felli, R. (2015), "La durabilité ou l'escamotage du développement durable," *Raisons politiques* 4(60): 149-160.

Fijalkow, Y. (2007), "Sociologie des villes," *Repères sociologie*. C. La Découverte.

Floridi, L. (2012), "Big data and their epistemological challenge," *Philosophy & Technology* 25(4): 435-437.

Foucault, M. (1975), *Surveiller et punir. Naissance de la prison*, Paris, Gallimard.

Gendron, C. (2014), "Penser l'acceptabilité sociale : au-delà de l'intérêt, les valeurs," *Communicate*, pp. 117-129.

Germain, A. (1997), "L'étranger et la ville," *Canadian Journal of Regional Science* Spring, summer: pp. 237-254.

Goffman, A. (2009), "On the Run: Wanted Men in a Philadelphia Ghetto," *American Sociological Review* 74(3): pp. 339-357.

Goodman, B., Flaxman S. (2016), "EU regulations on algorithmic decision-making and a 'right to explanation,' presented at 2016 *ICML Workshop on Human Interpretability in Machine Learning (WHI 2016),* New York, NY.

Goodman, B. (2016), "A Step Towards Accountable Algorithms? : Algorithmic bias and the European Union

General Data Protection," *29th Conference on Neural Information Processing Systems (NIPS 2016),* Barcelona, Spain.

Greenfield, A. (2014), "The truth about smart cities: 'In the end, they will destroy democracy,'" *The Guardian*. Viewed at: https://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase

Grieu, É. T., A. (2005), "La promesse à la source des relations interpersonnelles et sociales," *Revue d'éthique and théologie morale* 236: pp. 55-76.

Harvard Law School, et al. (2017), *The Future of IoT: Summary report*. Harvard Law School, in partnership with the Knight Foundation.

Haggerty, K. D. and Ericson, R.V. (2006), *The New Politics of Surveillance and Visibility*. Toronto*, University of Toronto Press*.

Heisenberg, W. (1990), *La Partie et le Tout - Le Monde de la physique atomique*. Paris, Flammarion.

Herschel, R., Miori, V. (2017), "Ethics and Big Data," *Technology in Society* 49: 31-36.

Inspire (2015), *EU INSPIRE Directive for Spatial Data*. Available at: https://inspire.ec.europa.eu/Legislation/Spatial-Data-Services/580

Institut de la statistique du Québec (2015), "Les compétences en littératie, en numératie et en resolution de problems dans les environnements technologiques : des clefs pour relever les défis du XXIe siècle," *Rapport québécois du Programme pour l'évaluation internationale des compétences des adultes (PEICA)*, Québec, QC, Institut de la statistique du Québec: p. 247.

Metcalf, J. (2014), *Ethic Codes: History, Context, and Challenges*, draft, viewed at: https://bdes.datasociety.net/council-output/ethics-codes-history-context-and-challenges/. Viewed February 20, 2018

Kaplan, D. (2012), *Ta ville, trop smart pour toi,* viewed at http://www.internetactu.net/2012/10/02/ta-ville-trop-smart-pour-toi/. Viewed February 20, 2018.

Kerr, I. and J. Earle (2013), "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture privacy," *Stanford Law Review Online* 66(65): pp. 65-72.

Kitchin, R. (2014), "The real time city. Big data and smart urbanism," *GeoJournal* 79(1): pp. 1-14.

Kitchin, R. (2015), "Making sense of smart cities: Addressing present shortcomings," *Cambridge Journal of Regions, Economy and Society* 8(1): pp. 131-136.

Kitchin, R. (2016), "The ethics of smart cities and urban science," *Philosophical Transaction of the Royal Society* 374(2083).

Kitchin, R. (2016), "Thinking critically about and researching algorithms," *Information, Communication & Society*: pp. 1-16.

Kitchin, R. a. (2014), *The data revolution: big data, open data, data infrastructures & their consequences*, London: Sage Publications Ltd, 2014, ©2014.

Koolhaas, R. (2014), "My thoughts on the smart city," *Digital Minds for a New Europe,* European Commission.

Sweeney, L. (2013), "Discrimination in online ad delivery," *ACMQueue* 11(3).

Landorf, C. (2011), "Evaluating social sustainability in historic urban environments," *International Journal of Heritage Studies,* 17(5): pp. 463-477.

Larson, J. e. M., Surya, Kirchner, Lauren and Angwin, Julia (2016), *How We Analyzed the COMPAS Recidivism Algorithm.* Viewed at: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Viewed May 23, 2016

Le Galès, P. (1995), "Gouvernement des villes à la gouvernance urbaine," *Revue française de science politique* 45(1): pp. 57-95.

Lecomte, S. (2017), "Le droit à l'oubli numérique : regards croisés sur la législation applicable en Europe, au Canada et aux États-Unis," *CanLII Connecte*.

Mannermaa, M. (2007), "Living in the European Ubiquitous Society," *Journal of Futures Studies* 11(4): pp. 105-120.

Mantelero, A. (2014), "The future of consumer data protection in the EU: Rethinking the 'notice and consent' paradigm in the new era of predictive analytics," *Computer Law and Security Report* 30(6): pp. 643-660.

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.

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

Michaud, T. (2010), "La science-fiction : une culture de innovation globale," *Journal for Communication Studies* 3(1): pp. 171-180.

Mittelstadt, B. D. e. A., Patrick and Taddeo, Mariarosaria, Wachter, Sandra and Floridi, Luciano (July-December 2016), "The ethics of algorithms: Mapping the debate," *Big Data & Society*, https://doi.org/10.1177/2053951716679679

Mohanty, S. P., et al. (2016), "Everything you wanted to know about smart cities," *IEEE Consumer Electronics Magazine* July: pp. 60-70.

Monfaredzadeh, T., Robert Krueger, (2015), *Investigating social factors of sustainability in a smart city*. International Conference on Sustainable Design, Engineering and Construction, Procedia Engineering

Moreno, C. (2015), "Ville intelligente : citoyenne et connectée," *Raisonnance. Cahier de réflexion des maires francophones.* (6): pp. 8-12.

Morozov, E. (2014), "De l'utopie numérique au choc social," *Le Monde Diplomatique*. Viewed at: https://www.monde-diplomatique.fr/2014/08/MOROZOV/50714. Viewed February 20, 2018.

Morozov, E. (2015), "Résister à l'uberisation du monde," *Le Monde Diplomatique*. Viewed at: https://www.monde-diplomatique.fr/2015/09/MOROZOV/53676. Viewed February 20, 2018.

Morozov, E. (2015), "Le mirage numérique. Pour une politique du Big Data," Paris, *Les Prairies ordinaires*.

Morozov, E. (2016), "La Sécu selon Uber," *Le Monde Diplomatique.* Viewed at: https://blog.mondediplo.net/2016-09-16-La-Secu-selon-Uber. Viewed February 20, 2018.

Moscovici, S. (2014), *Psychologie Sociale*, Presses Universitaires de France.

Mossenburg, K., Tolbert, J. and Stansbury (2003), *Virtual Inequality: Beyond the Digital Divide*. Washington DC, Washington University Press.

Mumford, L. ((1937) 2000), "What is a City?" *The city reader*. R. T. e. F. S. Le Gates. London, Routledge.

Nachi, M. (2003), *Éthique de la promesse: L'Agir responsable*. Paris, Presses Universitaires France.

Narayanan A., H. J., Felten E.W. (2016), "A Precautionary Approach to Big Data Privacy," *Data Protection on the Move. Law, Governance and Technology Series*, L. R. Gutwirth S., De Hert P. Dordrecht, Springer. p. 24.

Conseil national du numérique (2013), "Citoyens d'une société numérique. Accès, littératie, médiation, pouvoir d'agir : pour une nouvelle politique de l'inclusion," *Rapport à la Ministre déléguée chargée des petites et moyennes entreprises, de l'Innovation and l'Économie numérique*. Paris**:** p. 88.

Oddoux, A. (2016), "« Smart city » : de quelle intelligence parle-t-on?" *Blogue de Marco Cremaschi: Cycle urbanisme 2016-2017: Nos chroniques*. Viewed at: https://cremaschiblog.wordpress.com/2016/11/12/smart-city-de-quelle-intelligence-parle-ton-anais-oddoux/. Viewed February 20, 2018.

ODI (2015), *Open Data Certificate*, viewed at: https://certificates.theodi.org/en/. Viewed February 20, 2018.

Ohm, P. (2010), "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA L Rev*: 1701-1777.

European Parliament (2015), "Big data and smart devices and their impact on privacy," *Study for the LIBE Committee*. C. s. r. a. c. affairs, European Parliament.

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*, O. J. o. t. E. Union.

Pedreschi, D. e. R., S. and Turini, F. (2009), "Integrating induction and deduction for finding evidence of discrimination," *International Conference on Artificial Intelligence and Law* ACM**:** pp. 157-166.

Peres, É. (2015), "Les données numériques : un enjeu d'education and citoyenneté," *Journal officiel de la République française*. Avis du Conseil économique, social et environnemental**,** p. 154.

Picon, A. (2013), *Smart cities. Théorie et critique d'un idéal auto-réalisateur,* Paris, éditions B2.

Pisani, F. (2015), "Mais d'où vient cette idée bizarre de « ville intelligente » *? Le blog La Tribune*, 2017. Viewed at: https://www.latribune.fr/blogs/aux-coeurs-de-l-innovation/20150116trib4e9bdc2e1/mais-d-ou-vient-cette-idee-bizarre-de-ville-intelligente.html. Viewed February 20, 2018.

Plantard, P. (2013), "E-inclusion: Braconnage, bricolage et butinage," *Place publique* (Dossier: Faut-il avoir peur de la ville numérique ?), pp. 17-21.

Polonetsky, O. T. a. J. (2013), "Big Data for All: Privacy and User Control in the Age of Analytics," *Nw. J. Tech. & Intell. Prop* 11(239).

Poty, P. (2014), "Smartcities. Les clés numériques pour la ville intelligente," *Plateforme pour la Wallonie numérique*. Viewed at: https://www.digitalwallonia.be/smartcities-cles-numeriques-pour-la-ville-intelligente/. Viewed February 20, 2018.

McArdle, R and R. Kitchin (2014), "Improving the Veracity of Open and Real-Time Urban Data," *The Programmable Working City Paper*. p. 13.

Raley, R. (2013), "Dataveillance and Countervailance," *Raw Data Is an Oxymoron*, L. Gitelman, Cambridge, MIT Press**:** pp. 121-145.

Rallet, A. and Rochelandet, F. (2004), "La fracture numérique : une faille sans fondement ?" *Networks* 5(127-128): pp. 19-54.

Richards, N. M. (2013), "The Dangers of Surveillance," *Harvard Law Review* 126(1934): 1934-1965.

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

Ricoeur, P. (2000), *La Mémoire, l'histoire, l'oubli,* Paris, Seuil.

Romei, A. and Ruggieri, S. (2013), "Discrimination Data Analysis: A Multi-disciplinary Bibliography," *Discrimination and Privacy in the Information Society*. B. Custers, Calders, T., Schermer, B., Zarsky, T.; Heidelberg, Springer-Verlag Berlin.

Rouvroy, A. (2008), "Réinventer l'art d'oublier and se faire oublier in the société information?" *La security de l'individu numérisé. Réflexions prospectives et internationales*. S. Lacour. Paris, L'Harmattan**:** 249-278.

Rouvroy, A. e. Stiegler, B. (2016), "The Digital Regime of Truth: From the Algorithmic Governmentality to a New Rule of Law," *LA DELEUZIANA–ONLINE JOURNAL OF PHILOSOPHY*.

Rubinstein, I. S. (2013), "Big data: the end of privacy or a new beginning?" *International Data Privacy Law* **3**(2): pp. 74-87.

RUMPALA, Y. (2010), "Ce que la science-fiction pourrait apporter à la pensée politique," *Raisons politiques* 4(40): p. 93-112.

Sandovig, C. and K. Hamilton, K. Karahalios, C. Langbort (2014), "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms," *Data and Discrimination: Converting Critical Concerns into Productive Inquiry," at the Preconference of the 65th Annual Conference of the International Communication Association*. Seattle.

Sassen, S. (2010), *Talking back to your intelligent city*. McKinsey on Society, eds.

Schelings, C., Elsen, C. (2017), *Smart City concepts: from perception to acceptance,* 21st Conference of the Environmental and Sustainability Management Accounting Network (EMAN), Liège, Brussels.

Seth, S. (April 5, 2017), *In How Many Ways Can an Algorithm be Fair?* Viewed at: https://www.turing.ac.uk/events/many-ways-can-algorithm-fair-talk-visiting-researcher-suchana-seth/. Viewed February 20, 2018

Smolar, P. (2016), “Algorithmes sécrets de la surveillance israélienne en Cisjordanie,” *Le Monde*. Viewed at: http://www.lemonde.fr/international/article/2016/11/25/les-algorithms-secrets-de-la-surveillance-israelienne-en-cisjordanie_5037999_3210.html. Viewed February 20, 2018.

Söderström, O., et al. (2014), “Smart cities as corporate storytelling,” *City. Analysis of urban trends, culture, theory, policy, action* 18(3): pp. 307-320.

Solove, D. (2004), *The Digital Person: Technology and Privacy in the Information Age*. New York/London, New York University Press.

Stahl, B. C. (2011), “IT for a better future: how to integrate ethics, politics and innovation,” *Journal of Information, Communication & Ethics in Society* 9(3): pp. 140-156.

Stoycheff, E. (2016), “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring,” *Journalism & Mass Communication Quarterly* 93(2): pp. 1-16.

EDPS–European Data Protection Supervisor (2014), *Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy*. Brussels**:** p. 41.

Tavani, H. (2004), *Ethics and Technology: Ethical issues in an age of information and communication technology*. Hoboken, N.J., John Willey and Sons.

Taylor, A. (2014), *Démocratie.com*. Montréal, Lux.

Terrade, F., et al. (2009), “Social acceptability: How social determinants can influence analysis of technology system acceptability,” *Travail Humain* 72(4), pp. 383-395.

IERC—European Research Cluster on the Internet of Things (2015), *Internet of Things: IoT Governance, Privacy, and Security Issues*, E. C. I. S. a. Media. Brussels, European Commission: Information Society and Media.

Thomas, L.-V. (1984), *Fantasmes au quotidien*, Paris, Méridiens.

UNHCHR (2014), “The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights,” *Annual report of the UNHCHR and reports of the Office of the High Commissioner and the Secretary-General*. UNHCHR. Geneva, UNHCHR.

US EPA (2006), *Data Quality Assessment: A Reviewer’s Guide*, US EPA, Office of Environmental Information, Washington DC, February 2006.

Van den Hoven, J., et al. (2012), “Future ICT - the road towards ethical ICT,” *The European Physical Journal Special Topics* 214: pp. 153-181.

Van den Hoven, J. (2016), *Fact sheet - Ethics Subgroup IoT* - Version 4.0. E. Union.

Ville de Montréal (2017), *Montréal, smart city et numérique : Stratégie montréalaise 2014-2017*. Montréal, Ville de Montréal.

Walker, N.R. (2016), "American Crossroads: General Motors' Midcentury Campaign to Promote Modernist Urban Design in Hometown U.S.A. Buildings & Landscapes," *Journal of the Vernacular Architecture Forum,* Volume 23, Number 2, Fall 2016, pp. 89-115.

Wilson, W. J. (1987), *The Truly Disadvantaged: The Inner City, the Underclass, and Public Policy,* Chicago, University of Chicago Press.

Schwab, K. (2017), *The Fourth Industrial Revolution: what it means, how to respond*. World Economic Forum. Available at: https://www-weforum-org.proxy.bibliotheques.uqam.ca:2443/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Ziegeldorf, J. H. O. G. M. K. W. (2014), "Privacy in the Internet of Things: Threats and Challenges." *Security and communication networks* 7: pp. 2728-2742.

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
Supplement to Section on Privacy

Is Protecting Privacy Important?

Privacy is fundamental to the proper functioning of a society. By letting people keep information confidential, a society permits independent action, personal thinking and experimentation. Privacy nurtures diversity, development and the ability to cope with social pressures (Solove, 2006).

How Does the Public Feel About IoT-Privacy Concerns?

The 2015 TRUSTe US Consumer Privacy Confidence Index, indicated that 20% of online service users believe the benefits associated with the Internet of Things are more important than the privacy concerns they engender (TRUSTe, 2015). While these findings pertain to Europe and the Internet of Things involving common and personal objects (watches, medical equipment), they imply a very real anxiety with the general use of technology.

What Is Personal Data, in Terms of the Law?

The concept of privacy is related to that of personal data. Canadian legislation defines the latter as information about an identifiable individual, and in particular, information pertaining to a person's identity (race, religion, education, background, identifying data, address, as well as other criteria), his/her opinions or personal ideas and the ideas and opinions of other about him/her. For more information, visit: http://laws-lois.justice.gc.ca/fra/lois/P-21/.

What is the Theory of Contextual Integrity?

Helen Nissenbaum proposed that privacy is primarily based on the context in which information is exchanged, which gives rise to rules for such exchanges (Nissenbaum, 2004; Barocas and Nissenbaum, 2014). Information may or may not be shared without infringing on someone's privacy, depending on an interplay of multiple factors, including the parties' relationship, sensitivity of the information and direction of the exchange (two-way or one-way),[61] as illustrated in the following figure. Privacy is not an either/or situation, as it depends on context, rather than the kinds of information communicated. Nissenbaum (2014) consequently suggested that individuals might be entitled to privacy in a public space.

[61] This is called "the principle of contextual integrity" (Barocas and Nissenbaum, 2014). For example, rules on how information is used in a healthcare establishment determine what kinds of information can be shared by the parties concerned (patient, doctor, administrative staff, family). In this situation, patients who provide access to their personal information can do so, while maintaining their privacy, if the information is handled according to rules and social expectations pertaining to disclosure, sharing and confidentiality.

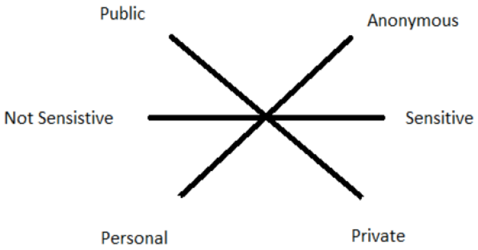


Figure 6: Contextual Privacy Factors (Gaughan, 2016, p. 17)

Are There Any Cases of Anonymized Data Being Re-Identified?

Acquisti, Gross and Stutzman (2011) demonstrated that it is now possible to ascertain a person's social insurance number using a photo of his or her face. Several studies by Sweeney (2000; 2013) also reveal the possibility of re-identifying individuals with public data. Meta- and geolocation data, it should be noted, play key roles in identifying individuals (Montjoye, et al., 2013).

There have been several cases where re-identified data that was released publicly was able to be re-identified, or where data that was assumed to have no identifying features could be correlated with specific populations. For example, in 2013, the New York City Taxi and Limousine Commission released a dataset of 173 million individual cab rides, and it included the pick-up and drop-off times, locations, fare and tip amounts. The taxi drivers' medallion numbers were anonymized (hashed) but this was quickly de-anonymized–revealing sensitive information such as any driver's annual income and enabling researchers to infer their home address (Franceschi-Bicchierrai, 2015). A data scientist at Neustar Research showed that by combining this data set with other forms of public information like celebrity blogs you could track well-known actors, and predict likely home addresses of people who frequented strip clubs (Tockar, 2014, in Metcalfe and Crawford, 2016). Another researcher demonstrated how the taxi dataset were devout Muslims by observing which drivers stopped at Muslim prayer times (Franceschi-Bicchierrai, 2015).

What Are the Basic Principles of Privacy by Design?

Privacy by Design involves: 1) Proactive (rather than reactive) solutions. 2) Privacy protection by default. 3) Privacy protection integrated into the design. 4) Full functionality, so systems can collect high quality data. 5) End-to-end security, throughout the entire life cycle. 6) Visibility and transparency. 7) Respect for user privacy (user-centred system design) (Gaughan, 2016, p. 57).[62]

[62] Note to self—SRG: Privacy by Design -14 (Ann Cavoukian, *Privacy by Design. From rhetoric to reality.* 2014).

Strategies Proposed for Transcending the Limitations of Anonymization

The literature provides several solutions for transcending the limitations of anonymization, including:

- Organizational commitment not to re-identify data.
- Aggregate (coarse-grained) data collection.
- Minimized data collection.

In its 2015 recommendations, the Federal Trade Commission suggested that companies keep their data in de-identified form (FTC, 2015) and implement mechanisms to ensure long-term data de-identification. According to this approach, businesses should: 1) Take reasonable measures to de-identify data. 2) Make a public commitment not to re-identify data. 3) Enter into binding contracts with third parties that ban data sharing and include the commitment not to re-identify data (FTC, 2015). As Tene and Polonetsky suggested (2013), the FTC has moved away from a strategy focused on the degree of data identifiability to one built around organization's intentions and its commitment to prevent re-identification. This approach takes into account that fact that data is not simply private or non-private, but falls within a constantly redefined privacy continuum (Tene and Polonetsky, 2013). Means of curbing and monitoring possible redefinition must accordingly be found.

Another proposed alternative is collecting coarse-grained data (van den Hoven, 2012, p. 170). Gaughan (2016) gave an example of data collection systems that can be configured as part of a "local aggregation technology" to aggregate data at the source and eliminate storage of local disaggregated data that could be associated with individuals (Gaughan, 2016, p. 60). This approach helps reduce quantities of stored sensor network data, with aggregating algorithms transforming individual data into summary statistics, based on system designer settings (Gaughan, 2016, p. 60; Narayanan, 2016). Under such circumstances, no individual could be geolocated and in most cases, nodal aggregation statistics could meet the analytical needs of city governments.

Minimized data collection is also often recommended (Narayanan, 2016).

What New Approaches Are Being Considered for Protecting Privacy with Metadata?

Researchers funded by the European Commission are now working on implementing sticky flow policies that would enforce access and confidentiality policies using metadata to mark data streams. This could mean, for example, that data be marked with a security policy describing how it can be used and what conditions must be met before it can migrate to a new data processing unit (IERC, 2015, p. 52).

What Are Citron's Additional Recommendations (2010) on Automated Decision-Making?

Danielle Citron (2010) proposed a variety of additional mechanisms that could be applied, such as:

- Investing in training on unconscious bias and automation bias for employees using systems to make administrative decisions. Such training will help them become more critical of decisions made by such systems.
- Require user entities to provide detailed explanations of decisions made by automated systems, including computer-generated information and results.
- Require user entities to test system software regularly for bias and other errors (Citron, 2010).

Council for Big Data, Ethics, and Society's 10 Rules for Responsible Big Data Research

Ten rules for responsible big data research (Zook, et al., 2017)

Modeled on PLOS Computational Biology–the first five rules around how to reduce the chance of harm resulting from big data research practices. The second five focus on ways researchers can contribute to building best practices that fit their disciplinary and methodological approaches. Paper is from the Council for Big Data, Ethics, and Society, a group of 20 scholars from a wide range of social, natural and computational sciences.

1. *Acknowledge that data are people and can do harm: data represent and impact people*
2. *Recognize that privacy is more than a binary value: privacy is contextual [11] and situational [12], not reducible to a public/private binary. Privacy also goes beyond single individuals and extends to groups [10]. 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 [14,15,16]*
3. *Guard against the re-identification of your data [22] (Even data about groups (aggregate statistics) can have serious implication if they reveal that certain communities, for example, suffer from stigmatised diseases or social behaviour much more than others [27] Identify possible vectors of re-identification in your data (MORE HERE)*
4. *Practice ethical data sharing*
5. *Consider the strengths and limitations of your data. big does not automatically mean better*
6. *Debate the tough, ethical choices: "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" (Zook, et al., 2017, 5)*
7. *Develop a code of conduct for your organisation, research community or industry: as a means to cement 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: in times of emergency*
    (Zook, et al., 2017)

However, the field of research ethics is grappling with the inability of existing frameworks to deal with issues raised by big data and, more generally, Economy 4.0. Research on big data is not concerned with physical harm to people, but to issues of privacy and discrimination resulting from data analysis. This is beyond the usual scope of research ethics, which has been greatly influenced by the biomedical field. Such a framework also often focuses on how choices are made and consent is given during data collection. However, such choice and consent rules have not been effectively applied and, on their own, are no longer relevant. Furthermore, research with big data "It fundamentally changes our understanding of research data to be (at least in theory) infinitely connectable, indefinitely repurposable, continuously updatable, and easily removed from the context of collection" (Metcalf and Crawford, 2016).

What is Crawford and Schultz'S (2014) Procedural Due Process Solution?

In view of the limited protection offered by notice and consent rules during data collection, Crawford and Schultz (2014) suggested applying procedural due process to the use of data and metadata on individuals. This would avoid ex ante regulation (as occurs when notice is given and consent requested prior to collection), instead controlling analytical fairness and equity through arbitration.[63] Such a process requires the respondent to give notice on how data was processed and enable parties to file complaints. This approach is based on Danielle Citron's proposals (2010), in her article "Technological Due Process," on automated government systems and the risk they pose to freedom and property. Crawford and Schultz build on Citron's ideas to include predictive data analysis.

This system would require entities engaged in data analysis to state how the analyses are to be used, as well as to produce audit trails. Those involved in predictive data analysis would be responsible must responsible for "disclosing not only the type of predictions they attempt, but also the general sources of data that they draw upon as inputs, including a means whereby those whose personal data is included can learn of that fact" (Crawford and Schultz, 2014, p. 33).

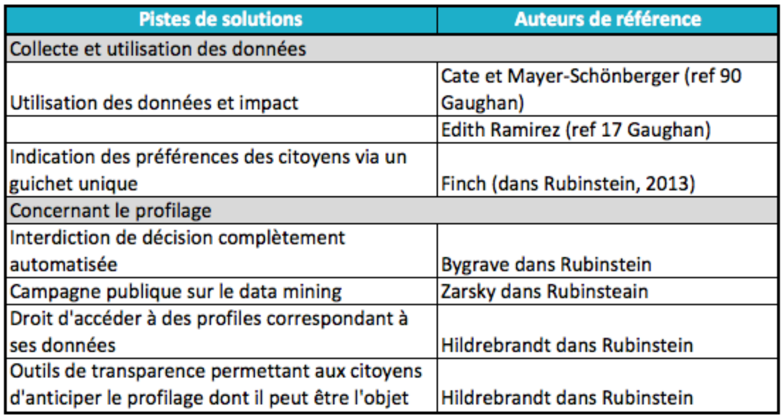
[63] There are seven enduring sets of values that due process should preserve: accuracy, appearance of fairness, equality of inputs into the process; predictability, transparency and rationality; participation; revelation privacy-dignity–each of these values maps well to our concerns about big data (Crawford and Schultz, 2014, p. 19).

What Other Possible Solutions Have Been Identified but not Explored in Detail?

Other Identified Potential Solutions Not Explored in Depth

The following table lists other potential solutions found in the literature review but not examined in depth (align references).

Table 2: Potential Solutions Identified but Not Explored



Pistes de solutions	Auteurs de référence
Collecte et utilisation des données	
Utilisation des données et impact	Cate et Mayer-Schönberger (ref 90 Gaughan)
	Edith Ramirez (ref 17 Gaughan)
Indication des préférences des citoyens via un guichet unique	Finch (dans Rubinstein, 2013)
Concernant le profilage	
Interdiction de décision complètement automatisée	Bygrave dans Rubinstein
Campagne publique sur le data mining	Zarsky dans Rubinsteain
Droit d'accéder à des profiles correspondant à ses données	Hildrebrandt dans Rubinstein
Outils de transparence permettant aux citoyens d'anticiper le profilage dont il peut être l'objet	Hildrebrandt dans Rubinstein

Appendix B
Privacy Principles

Existing North American privacy laws are largely based on Fair Information Practice Principles *(*FIPPs), governing the collection, use and dissemination of personal data (Richards and King, 2014; Schwartz, 1999). These five principles, initially known as the Code of Fair Information Practices Code, was established in 1973.[64] They are often summarized by such terms as openness, use limitation, individual participation (right to obtain/correct data), data quality and security safeguards and constitute the foundation of US privacy legislation.[65]

Table 3: Basic FIPPs

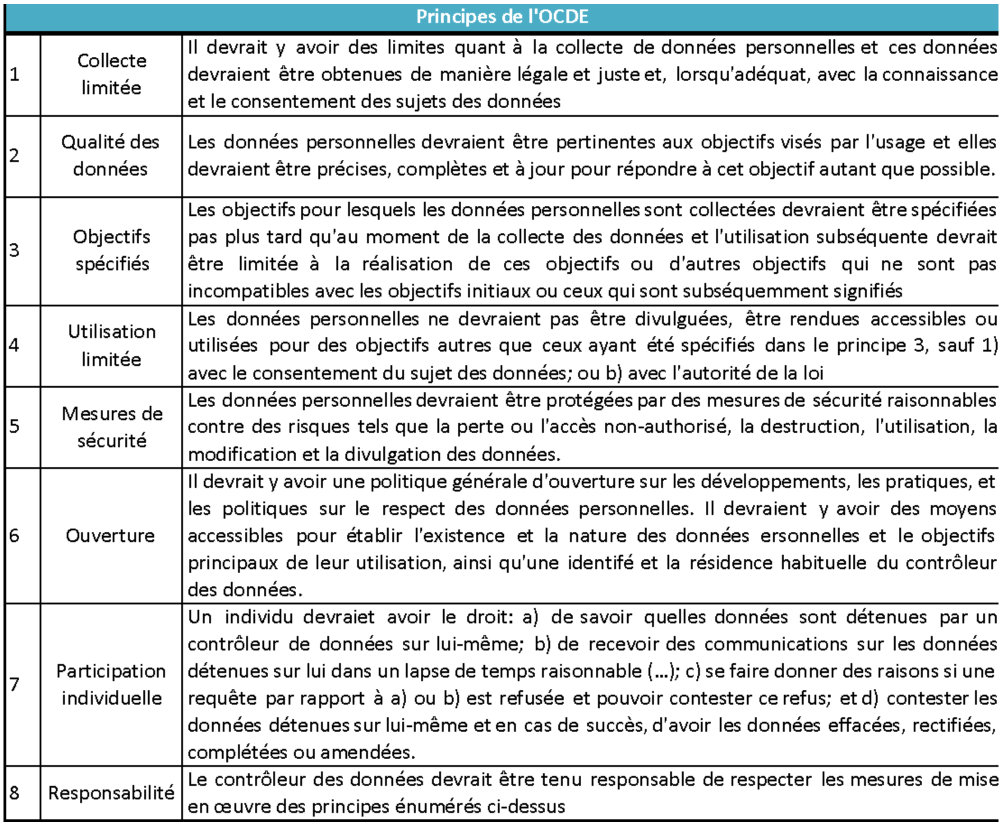
	Principes
1	Il ne peut y avoir de systèmes de tenue de registres dont l'existence est secrète
2	Il doit y avoir une façon pour une personne de trouver quelle information sur elle-même est tenue dans les registres et comment elle est utilisée
3	Il doit y avoir une façon pour une personne de prévenir que l'information sur elle-même qui a été obtenue pour une finalité soir utilisée ou mise à disposition pour d'autres finalités sans le consentement de la personne en question
4	Il doit y avoir une façon pour une personne de corriger ou amender un registre d'information identifiable sur la personne
5	Toute organisation créant, maintenant, utilisant ou disséminant des registres de données personnelles identifiables doit assurer la fiabilité des données pour leur utilisation prévue et doit prendre des précautions pour prévenir des mauvaises utilisations des données

OECD Guidelines on the Protection of Privacy and Transborder Flows of Data are a second cornerstone of privacy protection principles and the basis of most Western national and regional data privacy regulations, especially in Canada (Cate, 2006). These guidelines take a new approach by considering how data is used, and not merely how it is collected. As Table 4 illustrates, the reasons for using data and limitations on such use, appear next to the FIPPs (transparency; limits on data collection and access; monitoring the data; quality and security).

[64] As part of the 1973 report entitled *Records, Computers, and the Rights of Citizens,* by the US government's Advisory Committee on Automated Personal Data Systems.

[65] Another key privacy document was produced by the Private Protection Study Commission during Jimmy Carter's presidency in 1977. We do not discuss this document in detail here, since its highlights and those of the FIPPs were subsequently incorporated in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Data*.

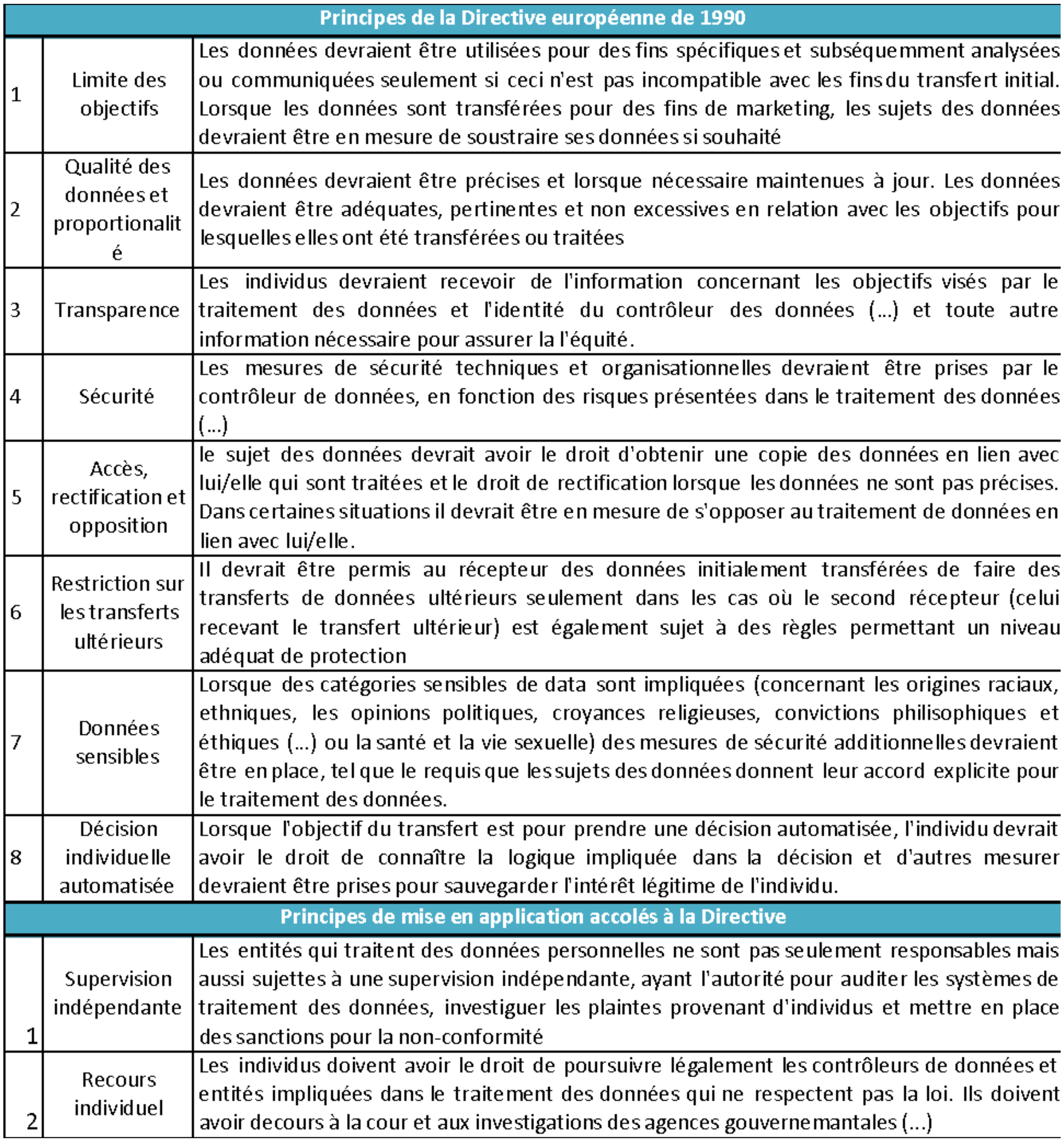
Table 4: OECD Guidelines



Principes de l'OCDE		
1	Collecte limitée	Il devrait y avoir des limites quant à la collecte de données personnelles et ces données devraient être obtenues de manière légale et juste et, lorsqu'adéquat, avec la connaissance et le consentement des sujets des données
2	Qualité des données	Les données personnelles devraient être pertinentes aux objectifs visés par l'usage et elles devraient être précises, complètes et à jour pour répondre à cet objectif autant que possible.
3	Objectifs spécifiés	Les objectifs pour lesquels les données personnelles sont collectées devraient être spécifiées pas plus tard qu'au moment de la collecte des données et l'utilisation subséquente devrait être limitée à la réalisation de ces objectifs ou d'autres objectifs qui ne sont pas incompatibles avec les objectifs initiaux ou ceux qui sont subséquemment signifiés
4	Utilisation limitée	Les données personnelles ne devraient pas être divulguées, être rendues accessibles ou utilisées pour des objectifs autres que ceux ayant été spécifiés dans le principe 3, sauf 1) avec le consentement du sujet des données; ou b) avec l'autorité de la loi
5	Mesures de sécurité	Les données personnelles devraient être protégées par des mesures de sécurité raisonnables contre des risques tels que la perte ou l'accès non-authorisé, la destruction, l'utilisation, la modification et la divulgation des données.
6	Ouverture	Il devrait y avoir une politique générale d'ouverture sur les développements, les pratiques, et les politiques sur le respect des données personnelles. Il devraient y avoir des moyens accessibles pour établir l'existence et la nature des données ersonnelles et le objectifs principaux de leur utilisation, ainsi qu'une identifé et la résidence habituelle du contrôleur des données.
7	Participation individuelle	Un individu devraiet avoir le droit: a) de savoir quelles données sont détenues par un contrôleur de données sur lui-même; b) de recevoir des communications sur les données détenues sur lui dans un lapse de temps raisonnable (...); c) se faire donner des raisons si une requête par rapport à a) ou b) est refusée et pouvoir contester ce refus; et d) contester les données détenues sur lui-même et en cas de succès, d'avoir les données effacées, rectifiées, complétées ou amendées.
8	Responsabilité	Le contrôleur des données devrait être tenu responsable de respecter les mesures de mise en œuvre des principes énumérés ci-dessus

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,* providing a roadmap to the adoption by EU members of national laws on the topic. It is particularly interesting that this directive focuses not just on personal data, but subsequent transfers of collected data (as for future third-party use) and automated decision-making, two issues not then covered by the principles discussed above. The following table summarizes the Directive's core principles and two important rules for use—independent monitoring (outside audit of data management and use, and personal recourse if harmed). The Directive is considered the most ambitious of all frameworks of this type, to date (Cate, 2006).

Table 5: 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 (...)

There is a final set of highly influential principles, which propose improvement in, rather than reduction of, existing rules. These are the privacy principles published in 1998 by the Federal Trade Commission, an independent US agency responsible for enforcing consumer legislation and monitoring anticompetitive trading practices. These principles deal exclusively with online privacy:

- Notice: Web sites must give consumers clear and prominent notice of their content management practices. This is considered the most basic principle.
- Choice and consent: Web sites must let users choose how their personally identifiable data is used outside of the purpose for which the information was originally provided.[66]
- Access and participation: Web sites must give users reasonable access to information the site collects on them, including a reasonable opportunity to review, correct and delete it.
- Integrity and security: Web sites must take reasonable measures to protect the security of information collected from users.

Many observers have mentioned that the legislative framework and corporate practices over the past few decades have strongly emphasized the concepts of notice and consent, or the idea that users/consumers should become acquainted with and check the content-management practices of companies with which they deal and allow to transfer their data in exchange for a given service. This principle is now often accompanied by the user's ability to configure their privacy rules.

A new *General Data Protection Regulation* was adopted in April 2016 and has been in force since May 2018. It is aimed at restoring people's control over their personal data, while simplifying the corporate regulatory environment. While the Regulation reinforces certain principles, it continues to rely on the consent principle and incorporates the following concepts:

- Explicit, positive consent.
- Right to erase data (if possible).
- Right to personal data portability.
- Setting limits to automated forensic profiling.
- Default Privacy by Design.
- Notification of data breaches.
- Appointment by public and private organizations of a data protection officer.
- Mandatory impact assessments of any activities with possible privacy implications.
- Encouragement in developing codes of conduct (European Parliament, 2016; Wikipedia, 2017)

[66] However, as stated in its 2012 privacy report: companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. This principle applies equally to the Internet of Things (FTC, 2015, p. 55)

Appendix C

Solove's (2007) and Ziegeldorf's (2014) Privacy Principles

Many of the activities involved in running an urban IoT can infringe on privacy. The works of Ziegeldorf, et al. (2014) and of Daniel Solove (2007) are particularly useful in identifying possible tension points—the first work concerns the smart city and the second, the general issue of privacy.

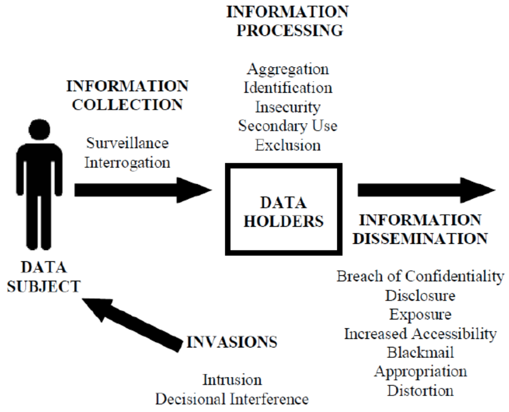
Daniel Solove's Privacy Classifications

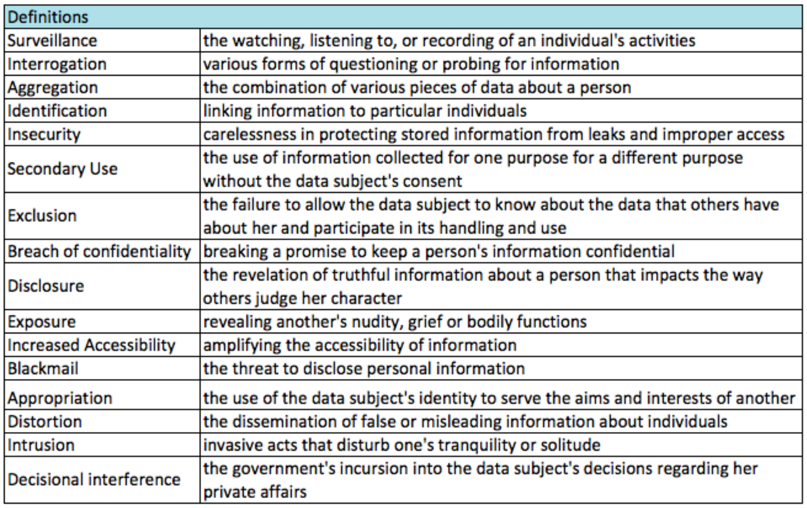
Daniel Solove (2007) proposed privacy classifications for identifying activities that are now socially recognized as violations of privacy, because they can harm individuals or they are likely to do so in the near term.[67] As presented below, these classifications are organized around four stages in data transit: 1) information collection, 2) information processing, 3) information dissemination and 4) invasion.[68]

[67] Solove's classification scheme has been greatly influenced by current US case law, but is also concerned with possible future infringements.

[68] The authors believe that the names of some of these activities, such as interrogation and exposure are not always intuitively clear, and in several instances quite different from expressions commonly used in the privacy literature. Their positions within the model are also sometimes surprising. The scheme remains useful, though, in acquiring a better understanding of privacy and issues that could infringe on it.

It should be noted that some of these activities, such as interrogation and exposure (see definitions of those terms beneath Figure 7), have little or nothing to do with urban IoT. Furthermore, some activities will not be administered by municipal agencies in the case of urban IoT, but by external parties interacting with the connected city.





Definitions	
Surveillance	the watching, listening to, or recording of an individual's activities
Interrogation	various forms of questioning or probing for information
Aggregation	the combination of various pieces of data about a person
Identification	linking information to particular individuals
Insecurity	carelessness in protecting stored information from leaks and improper access
Secondary Use	the use of information collected for one purpose for a different purpose without the data subject's consent
Exclusion	the failure to allow the data subject to know about the data that others have about her and participate in its handling and use
Breach of confidentiality	breaking a promise to keep a person's information confidential
Disclosure	the revelation of truthful information about a person that impacts the way others judge her character
Exposure	revealing another's nudity, grief or bodily functions
Increased Accessibility	amplifying the accessibility of information
Blackmail	the threat to disclose personal information
Appropriation	the use of the data subject's identity to serve the aims and interests of another
Distortion	the dissemination of false or misleading information about individuals
Intrusion	invasive acts that disturb one's tranquility or solitude
Decisional interference	the government's incursion into the data subject's decisions regarding her private affairs

Figure 7: Daniel Solove's Classification Scheme (2007)

Ziegeldorf's Diagram of Threats to Privacy

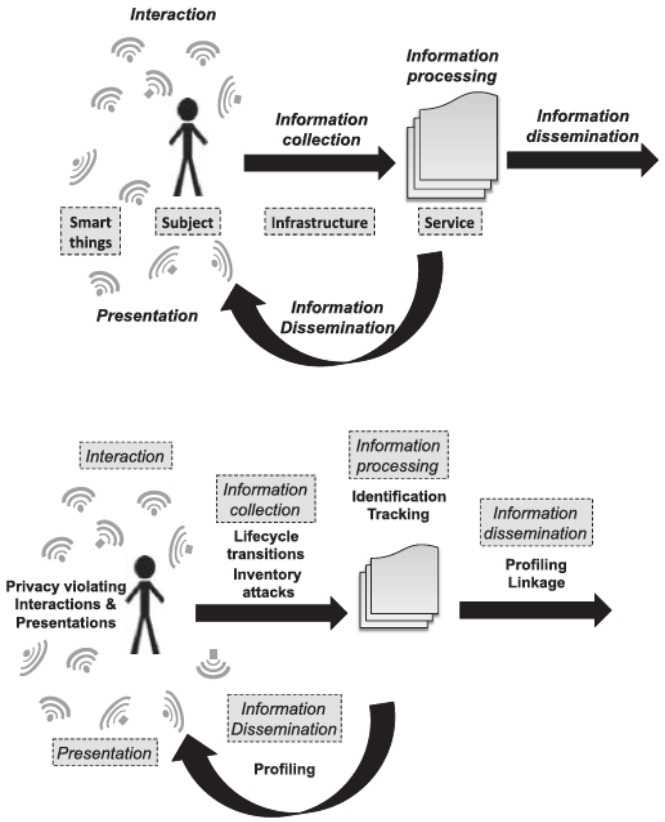
As appears in Figure 8, Ziegeldorf, et al. (2014) used a model[69] similar to the one of Solove (2007), with two new features: 1) Interaction between sensors and people during initial data generation. 2) Dissemination of information, after processing and analysis, to individuals.

Their model identifies:

- 4 entities: sensors, people, data collection infrastructure and data-processing services.
- 5 different kinds of information streams: initial interaction between people and sensors; information collection; data processing (analysis), generation of new information and services; dissemination of information to third parties (including people); presentation of services created to recipients.[70]
- 7 possible threats to privacy.

[69] Reference inspired by the Telecommunications Workers Union (TWU), as well as the model developed by the European Research Cluster on the Internet of Things (IERC)

[70] Ziegeldorf, et al. (2014) have identified other models, such as iOT-i consortium [18], Atzori, et al. [5], EU FP 7 projects IOT-A [19] and CASGRAS [20].



Definitions	
Identification	Associer un identifiant persistant (ex: nom, adresse) avec un individu ou des données à son sujet
Tracking	Déterminer et enregistrer la localisation d'une personne à travers le temps et l'espace
Profiling	Compiler un dossier d'information sur des individus pour inférer des intérêts par corrélation avec d'uatres profils et données
Privacy-violating interaction	Partager de l'information privée à travers un média public, à un public non souhaité
Life cycle transition	capteurs divulguent de l'information privée durant des changements de sphères de contrôle dans leur cycle de vie.
Inventory attack	Collecte d'information non authorisée
Linkage	Relier différents systèmes auparavant séparés de façon à ce que les données révèlent de l'information que le sujet n'a pas révélé avant et ne voulait pas révéler

Figure 8: Model of Ziegeldorf, et al. (2014)[71]

[71] Greater effort should be applied to understanding the transition life cycle concept fully.

Appendix D

Supplement to Section on Social Inclusion

Québec's Statistics for Literacy, Numeracy and Problem Solving in Technology Rich Environments (PSTREs)

There is a big digital divide in Montréal and throughout Québec. According to data from the Institut de Statistique de Québec (2015), some one in five Quebeckers have low levels of literacy and numeracy.[72] Fifty-one percent of the population has a very limited ability to interact with the digital environment.[73] While respondents of limited and very limited ability were still able to navigate the Web and perform simple tasks on an electronic device, they were quickly stumped by more complex operations, like backing up data and completing online forms. The Institut also noted that 17% of survey respondents did not have their PSTRE abilities assessed and profiles of that subgroup's members suggest the large majority have low PSTRE scores. The study also reported that 83.6% of Montréal households were connected to the Internet in 2012.[74]

Reference: http://www.stat.gouv.qc.ca/statistiques/science-technologie-innovation/utilisation-internet/menages-individus/menage-internet-2012.pdf

Discrimination and its Relationship to Algorithm Analysis

We should discuss the concept of discrimination, in addition to that of inclusion. As we know, stereotypes and prejudices are two characteristics of discrimination, which are both forms of collective profiling which outweigh reasoning in establishing characterizations of others (Amossy, 1989). An algorithm is "discriminatory" if its intrinsic logic includes stereotypes and prejudices. In the social sciences, algorithms are "artifacts" associated with social practices. Algorithms are never considered in and of themselves (Hegel), but perceived within a context of the algorithm and social practices.

Stereotypes are crude, oversimplified and rigid characterizations of an object or group. They are collective, pre-established, socially oriented and employed almost instinctively and routinely (Moscovici, 2014). They are decision-making habits not rooted in evidence, which every society conveys to its members through the family, social circles, school and media. Essential thinking—or explaining other people's conduct and behaviour in terms of their "essence" or "nature"—gives rise to stereotypes.

[72] "Low" means "inferior" and Level 1 of the ISQ evaluation scale.

[73] "Very low" means "inferior" and "low" means Level 1 of the ISQ evaluation. Please see Appendix for details.

[74] http://www.stat.gouv.qc.ca/statistiques/science-technologie-innovation/utilisation-internet/menages-individus/menage-internet-2012.pdf

Ambrose Bierce[75] defined prejudice, on the other hand, as "*a vagrant opinion without visible means of support,*" or, more simply, an unsupported claim. The Larousse defines prejudice as "*a pre-established judgement about someone or something based on various personal criteria and that positively or negatively influence feelings toward this person or thing, as in being prejudiced against someone or having an unfounded opinion, often imposed by society or school: Having the prejudices of his class.*"

Stereotypes and prejudices are used to categorize people. Categorization is a mental process of organizing and storing information on the living environment. Creating categories structures the world and gives it meaning. The process of categorization relies on a simplification of reality, emphasizing the similarities between elements of one category and the differences between categories.

Categorization in social psychology is used in studying social relations. In algorithm analysis, categorization is used to profile a person or a segment of the population. This means studying how encapsulation creates perceived categories, or put another way, the *partial hierarchies* that algorithms establish among people, groups and organizations (Brey and Soraker, 2009; Wiener 1988).[76] This process makes it easier to understand the kind of negative or positive bias algorithms tend to produce.

Antoinette Rouvroy[77] wrote that, in the past, statistics were generated through the creation of categories—categories arising out of academic, technical and political discourse and the testing of ideas, following by data collection surveys. Now, however, she said that categories come into being simply because data is available. She believes this will necessarily lead to schematization of the world, with the imminent emergence of digital reality governance. In other words, we are changing our system of governance by making what is currently visible obscure.

Strategies in the Literature for Promoting Public IT Education and Access

Multiple observers have recommended promotion of digital education (Peres, 2015). France's Conseil économique, social et environmental (CESE) has proposed that its e-inclusion policy should be developed as part of a broad-based, ongoing public initiative, and irrevocably linked to social inclusion. These proposals include:

[75] *The Devil's Dictionary* is a satirical lexicon with ninety-nine definitions written by Ambrose Bierce from 1881 to 1906.

[76] Brey, P and Soraker, JH, *Philosophy of Computing and Information Technology*, Elsevier, 2009; Wiener, N, *The human use of human beings: cybernetics and society*, Da Capo Press, 1988.

[77] Antoinette Rouvroy, Human Genes and Neoliberal Governance, Routledge-Cavendish, 2007.

- Promoting access to broadband technologies and Internet.
- Supporting the family's role in teaching children and young people.
- Promoting continuous education in school, from kindergarten through graduate studies.
- Encouraging the deployment/reinforcement of Wi-Fi access points and education for adults no longer in school.

All advances in digital education should naturally go hand-in-hand with progress in basic literacy and numeracy abilities. Peres (2015) suggested providing digital education on a variety of technologies, not just to acquire technical proficiency in using such resources, but to develop training that will promote the critical use of such technologies and education on personal data protection (Peres, 2015). In the same vein, others have recommended not focusing on the use of resources, but on enriching instrumental abilities (handling hardware and interfaces), as well as creative and productive skills (Conseil national du numérique, 2013). CESE recommends basic IT education focusing on a variety of technologies that familiarize students with three basic computer concepts: code, information and algorithm.

All of these approaches reflect the Conseil national du numérique's recommendation (2013) that "individuals should become knowledgeable and responsible users of digital data and not mere consumers and that use of such data not be the sole prerogative of business and government" (Conseil National du Numérique, 2013, p. 5).

Support networks have been suggested for deploying/reinforcing Wi-Fi access points and education, since issues of digital inclusion will now affect the entire population and we are aiming at a moving target—those comfortable with today's digital systems may be out of their depth, tomorrow, as these systems evolve and due to changes in use and goals of such use. Furthermore, while digital functionality is generally growing, the digital realm is constantly expanding and increasing in complexity. However, the people who have the greatest needs for such networks are those least likely to find a job, in a vulnerable situation or most disadvantaged (Conseil National du Numérique, 2013).

Digital education will also benefit if it is not treated as a "catch-up act," but a form of education contributing to personal/social development and creativity. The digital world can help people restore their self-esteem, eliminate their social exclusion, forge new social networks, stimulate creative behaviour, develop coordinated initiatives and facilitate democratic change (Conseil national du numérique, 2013).

Appendix E
Supplement to the Social Inclusion Section

Ethical Issues Posed by Algorithms, According to Mittelstadt, et al. (2016)

Table 6: Extract of an Article by Brent Daniel Mittelstadt, et al. (2016)

The six ethical challenges that algorithms pose to decision-making	
Lack of evidence or inconclusive reasoning	The term employed in the digital sphere is "actionable insight," which refers to an intuition, myth or belief that is sufficiently convincing for the decision-maker to take action even though the cause-and-effect link remains to be demonstrated.
Incremental evidence	If data has been used (or produced) as evidence in making a statement. Normally, if the relationship between the data and conclusion is unclear, additional arguments should be developed. However, algorithms are not well suited to the task. It ultimately becomes very difficult to explain the origin of data and its use in producing a statement.
Erroneous evidence	Reliability is entirely dependent on data quality. If the data is erroneous, the conclusions will be, too.
Unfair results	Actions taken based on algorithmic recommendations also possess an ethical component. Please see COMPAS software.
Transformative effect	The algorithm alters mental and social classifications, creating new meaning. This is why we refer to "algorithmic governance," since it modifies social structure.
Responsibility	If a technology fails, penalties should apply proportional to the damage caused. However, it is difficult to identify those responsible in the case of machine-learning algorithms because "*nobody has enough control over the machine's actions to be able to assume the responsibility for them*" (Matthias, 2004: 177).[78]

[78] Matthias A, "The responsibility gap: Ascribing responsibility for the actions of learning automata," *Ethics and Information Technology* 6(3): pp. 175-183, 2004.

Questions the US EPA Recommends Asking Before Publishing Environmental Data

The US Environmental Protection Agency established a list of four questions to ask before publishing environmental data, to permit data users to evaluate its quality and determine if it corresponds with the purposes for which it is being used (US EPA 2006). They are:

- Can the decision or estimate be produced with the desired level of certainty in view of data quality?
- What is the survey plan’s performance?
- If the same survey design strategy is used again for a similar study, should we expect the data to support the same uses with the desired level of certainty?
- Have enough samples been taken to permit a reviewer to see an effect if it is actually present? (US EPA, 2006)

Appendix F
Supplement to the Section on Freedom

Lifelogging

“Lifelogging” is the accumulation of quantitative personal data pertaining to multiple aspects (health, relationships, sports performance, etc.) of a person’s life. Various sensors and apps (such as connected watches), enable a lifeblogger to acquire “self-knowledge through numbers,” or in other words, personal statistics s/he can then analyze and share (Lupton, 2016). Lifelogging is a digital activity involving automated, continuous and cumulative “archiving” of routine activities in the form of digital data (images, graphics, geographic maps). This personal archive contains multimodal data obtained through generally ubiquitous digital tools (sensors plus apps). These systems record all events, conversations, texts, audiovisual data, and traces generated by sociodigital media, as well as biological data generated by sensors worn on the body, primarily to provide access to data and then cross-match it at a future time (Kelly, 2007; Dodge and Kitchin, 2007). Big data produced through lifeblogging, often with “freeware,” can usually be sold.

Subveillance

Bauman and Lyon refer to “mini-panopticons” that exist on a personal level. In addition to being monitored by third parties, everyone monitors themselves and others. In interacting with others, each person plays a kind of supervisory role (by taking pictures, recording conversations and capturing different data). “Subveillance” is the name occasionally used for such surveillance conducted–sometimes unintentionally–by the public itself, using personal digital devices (Mann, 2002) and complements institutional surveillance (Dodge and Kitchin, 2007). Such dataveillance is all the more pervasive because it takes forms that had never previously been suspected of serving such purposes. Such examples as gamification (increasing a technology’s social acceptability by applying typical elements of game playing to it), social interactions on digital social networks and digital reputation management can entail different types of autosurveillance arising out of compliance with various standards.

Predictive Consequence Analysis

Such forecasts are designed to minimize risk by predicting the consequences of a person’s actions. This could involve encouraging individuals to behave in ways best corresponding to their interests (often financial). For example, digital apps can be used to encourage a “poor” person not to become any poorer by reducing poor decision-making (Morozov, 2015).

This first type of forecasting is based on behavioural economics and nudging principles and is correctly found by some observers to be adversely paternalistic (Morozov, 2015). As laudable as these purposes may seem initially, consequence prediction infringes on personal autonomy, self-determination and privacy, and more broadly results in the government's shedding responsibility for policy, as well as for social and community discourse. In other words, rather than thinking collectively about problems and their causes in terms of contextual, historical, social and political issues, this process is usually handed over to businesses and mined for information without regard to underlying causes.

Appendix G
Supplement to the Section on Social Acceptability

“Social Acceptability” Defined in the Literature

The definition offered by Caron-Malenfant and Conraud (2009), authors of the “Guide pratique de l’acceptabilité sociale : pistes de réflexion et d’action,” is frequently cited in Québec and describes social acceptability as “the result of a process in which the parties concerned work together to create the minimum conditions needed to harmoniously integrate a program or policy at a given moment, within its natural and human environment.” This definition underscores social acceptability’s core principle and demonstrates that social acceptability is a co-construction that considers a wide range of opinions. It can be assumed that the solution ultimately implemented is the result of some compromise.

Beck (2001) proposed another widely used definition of social acceptability as “the anticipated acceptance of a short- and long-term risks relating to a project or situation.” The concept of risk associated with this definition suggests that the degree of social acceptability depends directly on what a community believes are acceptable project risks in terms of their likeliness to materialize (CPEQ, 2015).

According to Gendron (2014), in “Penser l’acceptabilité sociale : au-delà de l’intérêt, les valeurs,” social acceptability is the “public’s consent to a project or decision based on the collective judgment that the project or decision is superior to known alternatives, including the status quo.” This definition, adapted from Brunsson (1996), focuses more on social acceptability as the result of a collective judgment involving informed choices, including an excellent understanding of potential opportunities, benefits and risks.

These considerations are also apparent in definitions by organizations working with major projects. BAPE, which is responsible for conducting public consultations, has defined social acceptability as “as a collective, evolving process that brings a large number of local and regional stakeholders into play. It does not take the form of general consent, but of a consensus of stakeholders arising out of consultation and discussion” (2014 in Battelier, p. 51), and assumes that clients and decision-makers can explain their projects and have them approved by or make them acceptable to the parties concerned. The PMI’s Web site says, “Social acceptability is a vital concept,” because “some projects elicit opposition that the project management team must take into account to ensure the desired results are achieved.” In this context, social acceptability is seen as a factor in the success of major projects.