ABSTRACT

Nowadays, the adoption of smart cities worldwide is accelerating the digital transformation of urban environments. Besides, a huge amount of data is being exchanged through the smart devices, networks, cloud infrastructure, big data analysis and Internet of Things (IoT) applications both in private and public sector. This exchange of data aims to provide better services and to ensure a good quality of life for citizens. However, the use of smart applications raises several concerns regarding the violation of data privacy. Various privacy-preserving approaches have been proposed in the literature treating specific aspects of privacy in smart cities environments. Hence, comprehensive mechanisms are needed towards protecting data privacy including privacy preferences of citizens, organizations privacy policies, and privacy laws and regulations. In this paper, we provide a review of recent work dealing with privacy in smart cities. Furthermore, we make a comparison between some of the most known privacy laws and regulations. The aim is to show the importance of legal compliance in the privacy preserving process. In addition, a case study is presented to show how these laws can be considered by the different stakeholders.

Keywords
Privacy law, Smart cities, Privacy policy, Privacy preferences, Privacy preserving approach

1. INTRODUCTION

Governments all over the world have been investing in technology as to transform their cities towards the so called Smart Cities. A Smart City is defined as that city which uses both information and communication technologies to make its critical infrastructure and offered public services to be more interactive, efficient and so the citizens could be more aware about them. Smart Cities are associated with huge production of data which is collected from several applications like smart home, smart healthcare, smart grids, smart mobility, etc [1]. Consequently, processing and storing this large amount of data rise serious privacy concerns regarding the different stakeholders involved in a Smart City ecosystem: citizens, service providers, operators and policy makers or local governments.

Thus, with all data being exchanged and the multitude of actors using this data for different purposes, controlling who can access personal data, for what goal, how it will be stored, where, and how it is secured are all important data governance questions that interest both governments and citizens.

Therefore, efficient mechanisms and approaches are needed to protect privacy of citizens. To this purpose, various privacy preserving approaches have been proposed in the literature. However, most of the existing work has dealt only with specific aspects of privacy, but a holistic approach to deal with the concerns of the different stakeholders is missing. Particularly, the compliance with relevant privacy laws and regulations.

In fact, most approaches that have proposed solutions for smart cities data privacy issues such as Secure and sMArter ciTIEs data management (SMARTIE) [2], Internet of Things project (IoT@work) [3] are mainly oriented towards technical aspects and legal obligations of stakeholders are not widely covered. Hence, in this paper we compare some of the most relevant privacy laws and regulations aiming to protect data privacy of citizens. The goal is to show the importance of considering legal compliance in a privacy preserving smart city approach.

Furthermore, it is important that citizens play an important role in ensuring their privacy protection. As specified in many privacy laws, such as the Moroccan Law 09-08 [4], every citizen has the right to be included in any action regarding his personal data. Thus, citizens privacy preferences need to be expressed in an easy and formal way as to be taken into account in case a conflicting situation against service providers policies takes place [40]. In this way, choosing a suitable language to formalize citizen preferences, service providers policies as well as privacy laws and regulations is a serious issue requiring a particular attention. For this aim, a survey of the main privacy languages is presented.

In order to reach our intent, we structure the paper as following : Section 2 explains the concept of privacy and presents major risks caused by the development of Smart Cities technologies. Also, this section provides a detailed description of the main privacy preserving approaches and their limitations. Then, we show in Section 3 the role of legal compliance to privacy laws and regulations through a
Table 1: Major Privacy Risks In Smart cities [7]

<table>
<thead>
<tr>
<th>Enabling Technology</th>
<th>Example of Smart City Apps</th>
<th>Example of Privacy risk</th>
<th>Possible Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubiquitous Connectivity</td>
<td>Smart Public services (ex Free WiFi access)</td>
<td>Browsing history and location tracking</td>
<td>- Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Strong authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Strong encryption of personal data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Data Minimization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
<tr>
<td>Smart Cards</td>
<td>Smart Mobility of citizens</td>
<td>Card number leaks information about citizen</td>
<td>- Do not store identifiers of smart cards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Authentication without identification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Anonymous/Pseudonymous Credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
<tr>
<td>Open Data</td>
<td>- Smart health</td>
<td>- Sensitive health information about citizens</td>
<td>- K-anonymity</td>
</tr>
<tr>
<td></td>
<td>- Smart economy</td>
<td>- Data about public transport usage</td>
<td>- Differential privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>Smart grid</td>
<td>Profiling via energy consumption</td>
<td>- Data Minimization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Secret sharing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Data anonymization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Differential privacy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
<tr>
<td>Intelligent Vehicles</td>
<td>Smart mobility</td>
<td>Location Tracking</td>
<td>- Data Minimization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Anonymous/Pseudonymous Credentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
<tr>
<td>Autonomous systems</td>
<td>Smart Public service (Surveillance)</td>
<td>Profiling, video and audio surveillance</td>
<td>- Data Minimization</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Encryption of wireless communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>Smart Mobility</td>
<td>Unknown location of data</td>
<td>- Internal and external Audit tractability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
<tr>
<td>Wearable Devices</td>
<td>Smart apps for citizens</td>
<td>Location Tracking</td>
<td>- Avoid storing Encryption keys on device</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Strong authentication</td>
</tr>
<tr>
<td>Sensor Networks</td>
<td>Smart Mobility governance (Operations center)</td>
<td>- Location Tracking</td>
<td>- K-anonymity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- L-diversity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enforce privacy laws</td>
</tr>
</tbody>
</table>

comparative study. Section 4 presents and discusses related work. Finally we conclude the paper and present the future work.

2. PRIVACY IN SMART CITIES

Cities and communities generate data through a vast and growing network of connected technologies that power new and innovative services ranging from applications that can help drivers find parking spots to sensors that can improve water quality. Such services improve individual lives and make cities more efficient. However, the creation of these smart services may also pose numerous privacy issues that require particular attention.

2.1 Privacy concept

In spite of the several attempts that have been made to define privacy, no universal definition could be created [5]. Still, several definitions link privacy with the persons’ desire of keeping his sensitive information secret, safe and under control without the interruption of others [6]. Therefore, due to its big impact on individuals’ behaviours, privacy is considered a fundamental right that must be accorded to all people from all ages. Each one has the right to keep his personal information private and control the disclosure of that information.

2.2 Privacy in Smart Cities: role, challenges and major risks

Many intelligent applications appear when the smart City paradigm is gaining popularity that serves to connect the real world with the cyber world. Smart city applications bring benefits to cities and communities in various aspects such as Mobility, Utilities, Buildings, Environment, Public Services, Governance, Economy, Health care, and citizens [7]. The innovation in the smart city does not firstly rely on applications but in the use of "enabling technologies".
groups those technologies into nine categories: Ubiquitous Connectivity, Smart cards, Sensor Networks, wearable devices, the Internet of Things, Intelligent vehicles, Autonomous Systems, Cloud Computing, and Open Data. These technologies in turn raise many challenges and issues in terms of privacy.

Table 1 presents some of the major risks that can threaten citizen privacy while using enabling technologies in a smart city ecosystem. Hence, Smart city data is vulnerable to information leakage and misuse without citizen knowledge and consent. This data can be information about citizen identity, health conditions, user location, etc.

### 2.3 Privacy policies, preferences and languages

In order to enhance the citizen trust and confidence in smart cities services, organizations need to formalize the ways that will be used to gather and manage the citizen's sensitive information into what it called privacy policy.

"A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the Personally Identifiable Information (PII) that it gathers and uses in the normal course of business" [8].

"PII is any information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context" [9].

Privacy policies, mostly written in natural languages, play an essential role in preserving citizen's sensitive information. In fact, these statements should reflect citizen's preferences (e.g., who can access, for which service, how their data must be used, for what purpose, etc.) and also comply with the existing privacy laws and regulations for a better protection of privacy [10]. Hereby, privacy policies have simultaneously to reflect the needs of citizens and service providers with a legal compliance. For this end, Privacy languages were designed to formalize privacy controls that both service providers and users want to express [11]. In the literature, many privacy languages have been proposed. Most of these languages were designed for specific intentions with specific features and characteristics [12].

A privacy preference language enables users to express their wishes over their own personal data, while a privacy policy language is used by service providers to express their privacy commitment [13]. Still, the majority of the privacy languages does not consider simultaneously user's preferences and service providers policies (see Table 2). Consequently, privacy languages such as S4P and PPL are needed to respond to these limitations.

The next subsection is a comparative study of current privacy preserving approaches and solutions in smart cities environments.

### 2.4 Current Privacy Preserving approaches and limitations

In this part, we compare some recent approaches suggested in smart city context. Our objectives from this comparative study are:

- **First**, to identify from the studied works those who consider the citizen as an active actor regarding his privacy preferences.

- **Second**, to discover the main techniques used to preserve citizen data privacy.

#### Table 2: Major Privacy languages

<table>
<thead>
<tr>
<th>Privacy Language</th>
<th>Date of Publication</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3P [14]</td>
<td>1997</td>
<td>Privacy policy language</td>
</tr>
<tr>
<td>Rei [16]</td>
<td>2002</td>
<td>Privacy policy language</td>
</tr>
<tr>
<td>XPref [17]</td>
<td>2003</td>
<td>Privacy preference language</td>
</tr>
<tr>
<td>AIR [18]</td>
<td>2008</td>
<td>Privacy policy language</td>
</tr>
<tr>
<td>PPL [19]</td>
<td>2009</td>
<td>Privacy policy and preference language</td>
</tr>
<tr>
<td>S4P [20]</td>
<td>2009</td>
<td>Privacy policy and preference language</td>
</tr>
<tr>
<td>Jeeves [21]</td>
<td>2012</td>
<td>Privacy policy language</td>
</tr>
<tr>
<td>A-PPL [22]</td>
<td>2013</td>
<td>Privacy policy language</td>
</tr>
<tr>
<td>P2U [23]</td>
<td>2014</td>
<td>Privacy policy language</td>
</tr>
</tbody>
</table>

- Third, to show how laws and regulations are integrated in the conception of legal compliance-oriented approaches.

- Finally, to identify limitations of these approaches, as to allow researchers the possibility to propose solutions.

The study is presented in table 4. Here are the different criteria:

- **Type of smart application or service:**
  Determine the type of smart application (smart health, smart transportation, smart home, IoT apps, etc).

- **Is regulatory compliance considered?**
  Specify whether privacy laws and regulations are considered or not.

- **Used techniques:**
  Present the different privacy protection mechanisms used (Encryption, anonymization, access control, etc).

- **Are citizen’s preferences considered?** Determine whether the approach takes into account citizen's needs as to enhance user trust and confidence in smart cities services.

Smart city solutions where citizens play an active role in data management are implicitly expected to preserve citizen's privacy and establish confidence on smart innovations in an urban environment [24]. Most of the privacy preserving approaches presented in table 4 do not support analysis of privacy issues from different perspectives (e.g., legal compliance, organisational, threat and mitigation, citizen's needs, etc). Some authors works respond to our suggested criteria where other only rely on privacy preserving techniques neglecting citizen’s needs and regulatory compliance. Citizen's lack of confidence for smart applications and their perception on how service providers store and manage their data coupled with the lack of transparency are obstacles to the
wide adoption of smart cities applications [10]. Hence, holistic approaches for privacy protection in smart cities environment respecting citizen's choices and opinions and dealing with legal issues are needed.

3. A COMPARATIVE STUDY OF MAJOR PRIVACY LAWS IN SMART CITIES

Privacy laws and regulations are a positive development for cities and citizens. They provide much needed clarity around the purpose of personal data collection, how the data is used and how long the data will be retained for. Furthermore, those rules give citizens more control over their personal data and put in place much better safeguards and rights for the different stakeholders. From a city perspective, being compliant to privacy laws builds citizen's confidence in the organization. Similarly, engaging with companies that are privacy law compliant provides trust that their organisation is a good data custodian. Consequently, it is fundamental for citizens to have enough knowledge of their rights and responsibilities. For this purpose, we provide in this section the most pertinent privacy laws and regulations. These regulations are first presented and then analyzed considering various criteria.

3.1 Overview of major laws and regulations

- **The United States case:**
  The United States (U.S) possesses about 20 domain specific or medium-specific national privacy or data security laws and hundreds of others laws among its 50 states [25]. These laws can be classified into three main categories: Federal, State and other laws. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is considered as one of the most important federal laws to protect patient’s ability to access their health information and also to protect that data from unauthorised access [26]. HIPAA rules are organized on six titles where each title regulates specific operations or actions. The title II is the one focusing on the security and privacy protection of patients Protected Health Information (PHI) [27].

- **Canada:**
  The main Canadian initiative protecting privacy is called the Personal Information Protection and Electronic Documents Act (PIPEDA). It is based on 10 major principles: Accountability, Identifying purposes, consent, limiting Collection, limiting Use, Disclosure, retention, Accuracy, Safeguards, Openness and individual Access [28].

- **European Union:**
  The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in the last 20 years. In 2015, an agreement was made between the European Parliament and the council of the European Union to develop the GDPR and implement it in May of 2018 [29]. In fact, the GDPR was introduced to provide a unified data protection law for the EU to replace all of the existing Member state provisions [30]. In addition, it provides guidelines on what organisations can and cannot do with their user's personal data. This personal data is any data that can identify a user including their name, sexual orientation, health data and political opinions [31].

- **Moroccan case:**
  In Morocco, personal data protection is governed by the law 09-08 of 18 February 2009 and by its implementation Decree number 2-09-165 of 21 May 2009 [32]. This act defines the rights of the data subjects, the obligations of the data controller, as well as the rules governing the transfer of data abroad. Besides, it establishes the National Personal Data Control and Protection Commission (CNDP) which is the authority responsible for applying and ensuring compliance with the Act 09-08 [4].

3.2 The comparative study presentation:

In order to compare the different privacy laws we consider the following criteria:

- **Protected Information:**
  Every Law covers a specific type of protected data.

- **Covered entities:**
  Every Law is applied to specific entities.

- **Notification of personal data breaches:**
  The breach in this context is a security incident in which personal data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

- **Data Portability:**
  Is the right that allows individuals to move, copy or transfer personal data from one IT environment to another in a safe and secure way.

- **Cross jurisdictional impact:**
  Organizations that have business partners in other countries may need to consider other privacy laws.

- **Penalties:**
  Penalties often results in case of non compliance.

Table 3 presents a comparative study of the most known privacy laws and regulations i.e. GDPR [29], PIPEDA [33] and HIPPA [34].

According to this comparative study, we deduce that most of the studied data protection laws aim to protect sensitive data and reflect the same basic principles of data protection: Collection limitation, purpose specification, use limitation, consent, etc. The main differences are in the way of using and transferring personal information, the kind of information protected, information accountability as well as the level of penalties in the case of non compliance. Indeed, a given country may allow access for certain type of data while other countries may forbid it. Consequently, privacy policies may change when we move data from one location to another or one country to another creating a conflicting privacy policies [40]. To clarify this idea, we consider an example of this situation in the next subsection.
3.3 Case study : Privacy laws and conflicting policies and preferences

In order to highlight the importance of privacy laws and regulations in privacy protection process, we consider the following example inspired from [24].

Like many city administrations in Europe, City Council (CC) is moving towards an open governance model by transforming its administrative and decision making process. One of the steps taken by the CC is to make a large amount of city data open and accessible through its open data web interface which can be exploited by its citizens and other businesses.

Due to cuts in the IT budget, the CC wants to reduce the development and maintenance budget and hence decides to deploy its open data system on a cloud platform using a pay as you use model. This cloud platform is owned by an American Cloud Provider (CP).

CC intends to update and enrich this open data on a daily basis. Therefore it outsources a web based application to a local Service Developer (SD). As a legitimate Service Developer, SD can use available city data and develops new applications for its business. In the SD policy we find :

“We can also use personal information for internal purposes such as auditing, data analysis and research to improve our products”.

Using S4P privacy language, we can express Service Developer policy as follows:

May-Query:

“SD says SD may use personal information for auditing, data analysis and research purpose?”

CC is concerned about privacy aspects and requires that the identity of citizen using this web application be hidden from CP and SD.

Alice is a citizen who use the web application and whose data will be stored in a remote server from the American Cloud Provider.

Alice preference is defined as follows:

“It is possible to use my personal information for administrative purposes”.

Using S4P, Alice preference can be expressed as follows:

May-assertion:

“Alice says X may use data for administrative purposes only”

So we have in this case several privacy conflicts :

- Between SD policy and Alice's preferences.
- Between CC privacy rules and SD policy.
- Finally, Alice's data will travel from EU to US. As a result, a conflict between European and American laws will take place.

Nearby, the management of privacy data in this case must at once :

- Comply with the EU GDPR Law.
- Comply with American privacy laws and regulations.
- Avoid any illegitimate exploitation of citizens behavioural patterns.
- Respect privacy concerns of citizens based on their privacy preferences e.g anonymised feedback.

To sum up, the diversity of actors involved in a smart city context lead to conflicts among privacy policies defined by these actors. Besides, the citizen could be confused about which privacy policy and regulation should apply especially with the transfer of his personal data from one country to another.

4. RELATED WORK AND DISCUSSION

In the literature, many works have been suggested as to study and compare specific approaches of privacy in smart cities environments but a comprehensive survey to deal with various privacy issues is missing.

This comparative study, by contrast, provides an analysis of privacy concerns from different perspectives (e.g., technical aspects, privacy languages, privacy regulations, privacy preserving approaches). In addition, it takes into account "citizens preferences” and "regulatory requirement” as major features in assessing the effectiveness of different privacy preserving approaches.

In [2], researchers highlight privacy issues related to IoTs in smart city context and present different privacy preserving solutions and on-going projects. However, other privacy aspects are not mentioned.

In [12] authors mainly investigated the state of the art in policy languages with security and privacy scopes.

In [40] A comparative study of the most known privacy laws and regulations for healthcare is proposed. The aim is to show the importance of these regulations in preventing possible conflicts among privacy policies.

In [41] authors present the four dimensions of privacy , their challenges, possible threats and propose solutions in smart city context. They also analyse different privacy regulations in place in Spain and Europe.

Authors of [42] proposed a comparative study of the European Union General Data Protection Regulation (GDPR) with the statues of the 50 US states.

In [43] authors provide an overview of existing privacy issues and current privacy protection strategies in smart cities. They also point out the importance of the transparency and self-control of personal data.

In [44] A detailed review of existing privacy enhancing technologies and their applications in the context of smart cities is presented.

5. CONCLUSION AND FUTURE WORK

As Smart cities Applications become more sophisticated and more personal data is collected from those applications, individual privacy life is becoming more and more at risk.

Various privacy preserving approaches have been outlined here, but the majority of them do not support analysis of privacy from different dimensions especially the regulatory compliance aspect which plays a vital role in protecting individual's privacy.

In fact, privacy rules and regulations need to be expressed in formal way in order to avoid any possible conflict between organizations privacy policies and citizen's preferences.

As a future work, we intend to design a new comprehensive, platform-supported approach for privacy protection in smart cities that considers privacy aspects from different stakeholders point of view and where citizens and laws play a major role.
REFERENCES


