WS #253
Smart Cities Initiatives and Public Policy
Towards a “data for good” approach
A New World of Data
Brazil and **Smart Cities**

**Current Scenario:**

- **Growing population in major cities**
  
  I. São Paulo (12.1 million)  
  II. Rio de Janeiro (6.5 million)  
  III. Salvador (3 million)  

- **Development and implementation of Smart Cities Initiatives**  
  
  I. Public Wi-Fi  
  II. Public Transportation  
  III. Public Parking  

- **Lack of a regulatory framework for data protection**
Case Study: São Paulo

Public Parking
Public Parking – Zona Azul

- Analog Era
  - Physical tickets
- Problems:
  - Hard to find licensed sellers
  - Counterfeiting
  - High number of Illegal sellers
Public Parking – Zona Azul

- Digital Era
  - Digital cards only
  - 14 phone apps accredited by the São Paulo Traffic Engineering Company (CET-SP)
  - Any company that complies with the public notice can be accredited by CET-SP
## Public Parking

<table>
<thead>
<tr>
<th>Perks</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No more counterfeiting</td>
<td>• Public notice is too vague in regard to data protection</td>
</tr>
<tr>
<td>• No more illegal sellers</td>
<td>• Government is not interested in developing other public policies w/ data acquired</td>
</tr>
<tr>
<td>• Easier to purchase*</td>
<td>• Lack of transparency in regard to the use of user data by the accredited apps</td>
</tr>
<tr>
<td>• More $ to public safes</td>
<td></td>
</tr>
</tbody>
</table>
Public Parking

Data required by CET-SP (in order for the system to function)

- Login Information
- ID number
- License plate
- UDID/IMEI (Phone ID)
- Timestamp – activated card

Data collected by the apps* (not all apps)

- Login Information
- ID number
- License plate
- UDID/IMEI
- Timestamp – activated card
- Geolocation
- Private Address
- Brand/Model of the vehicle
- Date of birth
- Name of user’s mother (?)
- Others...
Permitir que “Estapar” tenha acesso à sua localização enquanto você usa o aplicativo?

Não Permitir  Permitir

Clique aqui e confira todas as ruas que têm zona Azul e estacione tranquilamente.
Smart Cities and Data Protection Conundrum

How to enable...

Privacy and personal data protection as a basic right

Efficiency in provision of services and utilities via SC initiatives

Use of data for the improvement of public policies (“data for good”)

...without a federal data protection law?
Campaign “your city your data”
Rebuild the narrative on smart cities
Translating the debate of data protection
Reactive vs proactive
The backbone of Municipal Personal Data Protections

• Regulates personal data protection regarding to its use by the **public municipal administration** (very strict scope);
  
  • a.1) Private Public partnerships: data should be seen as an **asset for public politics and not as funding sources**;
  
  • Privacy enhancing technologies/PETs as a **differential** in the **public bindings**
  
  • **Active and Passive Transparency**: the management of personal data
    
    • public algorithms and audits
  
  • **Multistakeholder Municipal Council**: the major part is from civil society
Why should we think in Municipal Personal Data Protection Laws?

- Privacy as a political fact;
  - Creation of a narrative for engagement: data protection as critical for citizenship;
  - Supra political party agenda: left and right political parties: 05 (five) different congressman have signed the Bill

- The capabilities of doing lobby: decentralization of the debate

- Feedback between the federal and municipal level
Carlos Liguori – carlos.liguori@fgv.br
Research coordinator/ Grupo de Ensino e Pesquisa em Inovação (GEPI – FGV)

Bruno R. Bioni - bioni.bruno@gmail.com
Researcher/ Latin American Network of Surveillance, Technology and Society Studies (LAVITS)

(in his personal capacity)