SMIT STUDIES MEDIA INNOVATION TECHNOLOGY

VUB CHAIR DATA PROTECTION ON THE GROUND

in partnership with BNP PARIBAS

POLICY BRIEF #25

20 May 2019

Connecting the dots – smarter cities work together

Ine van Zeeland, Jonas Breuer, Rob Heyman, Nils Walravens, Jo Pierson

This policy brief addresses common challenges for smart city projects under the EU's General Data Protection Regulation. We discuss 'on the ground' realities that may imperil the protection of personal data: innovation strategies, technology push, open data and data sharing, and vendor lock-in. Based on imec-SMIT's extensive experience in smart city projects, we recommend early consideration of data protection in project planning, sharing budgets and lessons learned, carefully balancing citizen needs with technology push, coordinating tools and procurement, and overall: 'connecting the dots', closer collaboration.

1. Introduction

At imec-SMIT, the seat of the VUB Chair on Smart Cities, we take part in several smart city initiatives and investigate how their applicability and sustainability can be promoted. In our Smart City Meter 2018 survey[1], we found that citizens are more inclined to share data if their privacy is less affected. The results also show that citizens want to know what their data are used for and regard overly intrusive initiatives as useless. For example, fewer citizens accept surveillance cameras when those are capable of face recognition.

Echoing the increased public awareness of privacy issues, the European Union's General Data Protection Regulation (GDPR)[2] entails closer scrutiny of data protection in all organisations. This means that smart city initiatives are also increasingly held accountable for citizens' right to data protection. In this policy brief, we discuss challenges related to strategic choices, technology push, data sharing and open data, and vendor lock-in. We conclude by offering recommendations to the effect that collaboration will help resolve these challenges.

2. Strategic considerations for data protection

One challenge in smart city projects is deciding between an experimental, innovative approach on the one hand, or tried-and-tested solutions on the other hand. In experimental situations, cities bear innovation risks but can take ownership of solutions. Cities are directly involved in discussions with developers, legal specialists, and user researchers. If, on the other hand, cities select solutions 'off the shelf', innovation risks are delegated. Cities do not control choices in development, legal considerations and user interfaces. The technology is a black box to them and risks associated with data protection and privacy become opaque as well.

Technologies prescribe data processing scenarios, so if a city chooses a technology before it defines a project goal (see section 3 below), this limits data protection possibilities. For example, surveillance cameras offer no control to citizens: a citizen cannot choose not to be filmed when in range. A personal tracking device like a smartwatch offers more control, since a citizen can choose not to wear it or to turn it off. Smartphone apps can be deleted. In other words, different 'sensors' offer citizens different levels of choice and control. Levels of choice and control limit the options for legally processing personal data like camera images or location data under the GDPR. In this example, cameras and WIFI scanners are less suitable

[1] This annual survey is held among citizens in Flanders and Brussels in collaboration with imec City of Things and imec Living Labs. The Smart Meter 2019 survey is currently in progress. Find more information here: imeccityofthings.be/smart-city-meter

[2] Regulation (EU) 2016/679 https://eur-lex.europa.eu/CELEX:32016R0679

for consent or contractual obligations as the legal basis for processing personal data, while wearables and smartphone applications are more suitable for consent or contracts. City administrations should strategically consider these aspects before choosing a technology.

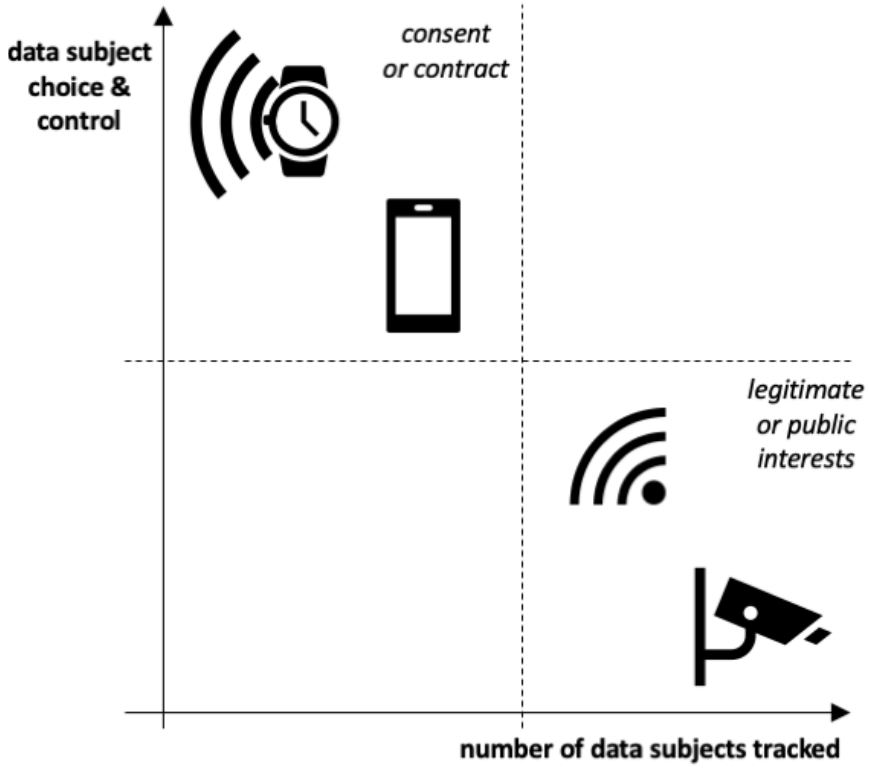

Figure 1 How technology choice affects the legal basis for processing personal data

Given the reality that large cities have more means to innovate than small cities, important strategic choices must be made above city level. Collaboration in innovative development is likely to be more cost-efficient than separate investments by cities in the same type of projects. On a national or regional level, the prevention of two-speed development must be considered, i.e. a situation in which large cities can weigh the pros and cons of technological choices for data protection, while smaller cities have no choice but to follow dictates of the market.

3. Balancing technology push with citizens' needs

The inspiration for smart city initiatives originates in new technological solutions and/or urban challenges or citizen concerns. While a project can balance innovation and challenges, most projects favour technological solutions. This tendency reminds us of an old innovation paradigm, 'technology push', which refers to a situation in which technology is taken as the starting point. For instance, a city may already have surveillance camera feeds and find new ways to use them, such as counting passers-by. When, on the other hand, a specific need requires a technological solution, this can be called a bottom-up demand (or 'market pull'). For instance, a city may need to count passers-by and seek a fitting technology. We have observed that data protection requirements can be more constraining in 'technology push' situations than in 'bottom-up' initiatives. After all, adapting technology and systems retroactively is more challenging than incorporating 'data protection by design'. The GDPR requires data processing operations to start from a purpose and define all means proportionally to that purpose.

Giving equal attention to 'push' and 'pull' therefore affords decisive advantages: the principles of necessity and proportionality underlying EU law, including the GDPR, entail that intruding on citizens' fundamental right to data protection is only allowed if necessary and proportional. Including citizens from the start can help match existing urban challenges with uses (and revenues) for a technology. Here, the 'living labs' approach is especially suitable for such user research in smart city innovation, because citizens become co-creators of technologies.[3] Two

[3] See e.g. Ballon, P., & Schuurman, D. (2015). Living labs: concepts, tools and cases. *info*, 17(4).

examples of such approaches that imec-SMIT is involved in are the ESSENCE[4] project and the 'Brussels by us'[5] initiative.

4. Open data and sharing data with partners

Under the 'open data' moniker, government organisations publish data in accordance with open standards and clear licenses. The aim is that other government organisations, companies and citizens can use these data to create new applications or insights.

Open data are not identifiable by definition; they refer to the environment, mobility, public space and so on. However, this does often include data about people: it is impossible to process traffic data or (land) property data without including any data about people. Therefore data are often de-identified: anonymised, pseudonymised, or aggregated. But because ever more datasets are published and tracking people is increasingly common, it is a matter of time until individuals are re-identified. For instance, de-identified taxi data, health data, and educational data were proven to be re-identifiable by combination with other open datasets. In response, more secure de-identification techniques have been developed, such as *k*-anonymity: a technique to 'hide in the crowd' by making sure that a minimum number of individuals in a dataset share the same characteristics, so it is never possible to uniquely identify one person.[6] Considering the need for such advanced 'privacy by design' techniques should be part of a standard assessment procedure before datasets are opened up.

Book recommendation (in Dutch):

Open Data: opportuniteiten en uitdagingen voor lokale besturen

Nils Walravens, Mathias Van Compernolle, Pieter Colpaert, Nathalie Dumarey

ISBN: 978-2-509-03355-0

Smart city initiatives are often public-private partnerships. A recurring tension in these partnerships has to do with control and access: all parties involved want to be data owners, but no-one wants the responsibilities of data controllers. While data ownership is a legally debatable idea, the GDPR is clear about data controllership: those who determine the purposes and means of personal data processing are controllers. In reality, there is hardly ever a single controller: many parties share some decision-making about the purposes and means of data processing. Joint controllership (Article 26 GDPR) seems the best solution. This means dividing responsibilities and clearly communicating those to citizens, so they will know where to ask questions.

A related issue is that government authorities cannot rely on 'legitimate interests' as a legal basis for processing citizen data, while companies cannot rely on the legal basis of 'public interest'. As a consequence, public and private partners may not be able to use one legal basis for processing personal data. Multiple agreements may be needed to process data from a single project, which will not improve the transparency of the arrangement. This issue may be addressed by finding ways to combine public interest assessments with legitimate interest assessments, preferably with support from the Data Protection Authority. Alternatively, the legal basis of 'consent from citizens' can be sought for all data processing purposes, but this can be complicated in some situations (see section 2 above).

5. Vendor Lock-in

Much of the ICT systems cities rely on are third-party services, even at the level of office software, e.g. Microsoft's Office 365 (a cloud service). In most cases, data and application are

[4] imec-int.com/essence
[5] brusselsbyus.be/
[6] *K*-anonymity was first introduced in: Pierangela, S. & Sweeney, L. (1998). *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression.*

sold as one proprietary package. This dependency on vendors causes problems for cities when they want to change providers without incurring prohibitively high switching costs or loss of data. Contracts often do not include specific provisions for ownership of the data, access to data, or usage rights. This 'vendor lock-in' has become deeply rooted in many Belgian cities. Relations with smart-city technology vendors must evolve to more balanced partnerships. To this end, the Smart Flanders project published example 'standard clauses' to support cities in negotiations with suppliers.[7] Using standard clauses across the thirteen cities in the project strengthens their position towards suppliers and avoids unclear formulations in contracts.

As was mentioned above for data sharing, procurement requirements should include an assessment of privacy-protective measures and 'privacy by design'. Referencing GDPR requirements and potential enforcement actions can strengthen the negotiating position of city administrators as well. According to the GDPR, citizens can request access to data about them (as well as correction and removal), meaning that data processing by third parties must be transparent. Moreover, to enable the GDPR-required data portability for citizens, data should be readable to other systems, which entails that switching vendors should also be less difficult for cities.

6. Recommendations

Based on the challenges discussed above, we recommend the following to smart city project managers, policy-makers, Data Protection Authorities, and regional and federal governments:

- **Consider personal data protection as early as possible**
  Whether initiatives are more experimental or more reliant on tested technologies, the analysis above shows that the earlier in the process personal data protection aspects are considered, the easier integrating them in technologies and systems will be.

- **Share budgets and lessons learned**
  The Flanders region should take into account the costs of taking the lead for smaller cities, or small cities will become consumers of off-the-shelf solutions with little or no control. Regional and national authorities should consider lining up efforts or allocating a larger part of the budget to smaller groups of cities that face similar challenges.

- **Balance citizen needs with finding uses for technology**
  Paying equivalent attention to bottom-up needs will prevent costly retroactive adjustments and improve accountability. This also involves careful consideration of how technology steers towards particular legal grounds for data processing.

- **Develop 'interests assessments'**
  As 'consent' is often not an ideal basis for processing citizen data, public interest assessments and legitimate interest assessments should be elaborated, and the possibility to combine both should be investigated. There is an important role here for Data Protection Authorities to provide clear delineations and guidance.

- **Draw up common tools, templates, and standard clauses**
  Following the example of standard clauses from the Smart Flanders project, common tools, templates and contract clauses for personal data protection in smart city projects across a region will level the playing field and improve clarity for all parties.

- **Prepare procurement with an eye on data protection**
  Pre-commercial procurement can alleviate the pain of power imbalances: rather than describing a desired solution in detail, governments should put a 'challenge' into the market with requirements on outcomes, including privacy-protective measures.[8]

7 The goal of the Smart Flanders project is to find common standards for the provision of open data (among other goals). Find all recommendations (in Dutch) here: http://smart.flanders.be.
8 An example of how this can be done is the SELECT for Cities project: https://www.select4cities.eu.

Book recommendation (in Dutch):

De humane stad
30 voorstellen voor een stad op mensenmaat

Pieter Ballon,
Cathy Macharis, Michael Ryckewaert

ISBN:
978-90-5718-704-9

About the authors:

Ine van Zeeland is a PhD researcher within the VUB research chair on Data Protection On The Ground.

Jonas Breuer is a PhD researcher at imec-SMIT, primarily involved in the SPECTRE project, which investigates the involvement of citizens in creating citizen-friendly and privacy-compliant Smart Cities.

Rob Heyman is a senior researcher at imec-SMIT, focusing on privacy and data protection. He is a leading researcher in Antwerp City of Things and the SPECTRE project.

Nils Walravens is a senior research at imec-SMIT, focusing on the role of technology in the urban context. He coordinates the Smart Flanders project and is responsible for several other projects related to smart cities and open data.

Jo Pierson is in charge of the research unit 'Privacy, Ethics & Literacy' at SMIT and associate professor in the Department of Media and Communication Studies at the Vrije Universiteit Brussel. He holds the VUB research chair on Data Protection On The Ground.

SMIT (Studies in Media, Innovation and Technology) is an imec research group at Vrije Universiteit Brussel. Our research focuses on three domains of digital innovation: Media, Cities, and Health & work. These three domains are approached with our expertise in living labs, market & policy, and privacy, ethics & literacy research.