



OCTOBER 2019

A smart Smart City plan: The importance of controlling the flow and storage of ‘the new coal’

This Policy Brief introduces the concept of ‘smart cities’ and raises a number of data security concerns for the Netherlands, particularly in relation to foreign ownership or foreign transfers of the collected data. Furthermore, it argues for a deeper understanding of the vulnerabilities created by smart cities and highlights a number of areas of further research in order to assess the extent to which Western companies are entangled with Chinese tech firms. The Netherlands must first ensure that it can safely store and secure Dutch citizens’ data before we switch to ‘smart’ cities.

Introduction

A Deloitte study from June 2018 estimated that there were about 1,000 smart city pilots worldwide, of which around 500 were located in China.¹ By comparison, the same study estimated a total of 90 smart city pilot projects in Europe and about 40 in the United States (U.S.).

A smart city is a city in which information technology, the internet of things (IoT) and artificial intelligence (AI) are used to manage and control the city. Not only the administration of the city, but also services such as libraries, hospitals, the transportation system and utilities are managed and controlled with information technology. One of the motives behind smart cities is to make cities safer and more efficient.

AI cameras, for example, can enable emergency services to reach the scene of an accident faster by detecting and analysing aggressive behaviour. However, there are also reasons to worry about the implications of these technological developments.

Smart cities thrive on access to – and accumulate – large quantities of data. This includes anonymous data, but also personal information, for example from licence plate recognition, the tracking of smartphones or the use of facial recognition technologies. Who will be allowed to collect, store and analyse this data and for what purposes? Data is perceived to be the new gold, but is perhaps better described as the new coal: fuelling the Fourth Industrial Revolution similarly to how previous Industrial Revolutions were powered by coal, electricity and combinations of automation, mechanization and computerization. How much of this precious resource is currently leaking out of the Netherlands through foreign companies? How do we

¹ Deloitte (2018). Super Smart City: Happier Society with Higher Quality. Available online at: <https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/public-sector/deloitte-cn-ps-super-smart-city-en-180629.pdf>.

make sure that the critical² data from our cities stays in the Netherlands and benefits Dutch citizens rather than harming them?

The leading AI firms and cloud service providers – worldwide and in the Netherlands – are currently mostly U.S. companies, which means that most Dutch data stored in the cloud is in the hands of U.S. companies. However, this is likely to change in the coming years as Chinese companies are on their way to becoming world-leading smart city technology firms. What will the growing dominance of Chinese smart city technology firms mean for the control of the data collected in Dutch smart cities? How intertwined are Dutch cities already with these Chinese companies? Who has access to and control of the data that is collected by U.S. and Chinese firms in Dutch smart cities?

The smart cities market

No clear and consistent definition of a smart city yet exists. However, Mohanty et al. have provided a rather simple explanation of this complex concept:

In a simplistic explanation, a smart city is a place where traditional networks and services are made more flexible, efficient, and sustainable with the use of information, digital and telecommunication technologies, to improve its operations for the benefit of its inhabitants.³

-
- 2 To know what data is critical, we only have to ask ourselves what data we would not want to see in the hands of the government of a non-friendly country or a criminal organization. The more critical infrastructure can be controlled remotely – or relies on digital systems – the higher the risk of a shutdown caused by a hack (see the example in Huib Modderkolk (2019) ‘Het is oorlog, maar niemand die het ziet’ on the danger of relying on digital certificates). Furthermore, the data collected in smart cities could be used by non-friendly countries or criminal organizations to trace (and kidnap, kill or blackmail) a person.
 - 3 Mohanty, S. P., Choppali, U. & Kougianos, E. (2016). Everything you wanted to know about smart cities: The Internet of Things is the backbone. *IEEE Consumer Electronics Magazine*, 16, p. 2162.

The most common smart city application segments are: mobility, home, healthcare, energy, water, waste, retail, governance, building, security and education. Examples are street lights that only switch on at night when they detect a person or vehicle on the street. This enables the city to save energy. These same streetlights can be equipped with wifi trackers that track the movements of passers-by and this information can be sold to the shop owners, who, for example, can then assess whether they are displaying their merchandise in an attractive way. These streetlights can also be equipped with cameras that use AI programs to detect potential dangerous behaviour and are connected to the emergency services to ensure a rapid response.

Most definitions of smart cities are ambiguous about the actors involved in these processes and their levels of agency. A smart city is not just a city that uses new technologies. It is a complex ecosystem made up of many stakeholders, including citizens, city authorities and local and foreign companies. It is important to realize that the smart solutions used in smart cities do not only benefit the inhabitants, but can also potentially harm them. Every step of every person in a smart city can be traced, watched and analysed. That not only limits privacy, but also poses a potential security risk if a company from a non-friendly country can trace the movements of the Prime Minister’s car, for example.

Smart city technology solutions: solving existing problems or creating new markets?

The term ‘smart city’ was coined by the industry when telecom and tech firms started to look for new revenue models during the last economic crisis, according to technology author Evgeny Morozov.⁴ The companies presented themselves as saviours of the

-
- 4 Naafs, S. (2017, 6 December). De muren hebben sensoren. In: De Groene Amsterdammer. Available online at: <https://www.groene.nl/artikel/de-muren-hebben-sensoren>.

cities while saving their own businesses. Smart cities are big business for companies that can provide the infrastructure for superfast internet, sensors, data processing and algorithms. Companies test their services in a city, improve them with the data they acquire in the public spaces and sell their services (and data) to other places. Meanwhile, access to large quantities of data is empowering these companies.

Albert Seubers, Director Global Strategy IT in Cities at ATOS, states that in order to maximize the value of smart technologies for citizens the municipality needs to have access to this data.⁵ He argues that monopolization of data must be prevented and the reuse of data should be maximized. However, this is currently not the case as different suppliers of technologies for smart city applications have their own cloud contracts.⁶ Are cities becoming too dependent on private companies? What is the situation in the Netherlands? Are the smart city developments in the Netherlands more government-, people- or business-driven? Who owns, stores and controls the data?

Dutch Smart Cities

In the summer of 2016 the Dutch Prime Minister Mark Rutte requested a vision for the direction for smart cities in the Netherlands. The resulting report “NL Smart City Strategie: The future of living” characterizes smart cities merely as a business model, a way to promote Dutch technology worldwide.⁷ The report describes the Netherlands as highly urbanized and argues that together with the global need

for sustainability it requires an innovative approach to increase the quality of life of citizens while seizing economic opportunities. The main advice to cities from this study is to upscale from dispersed initiatives (pilot projects) to large-scale projects and then export the accumulated knowledge. However, is the Dutch government also able to steer the direction for smart cities?

A research project by Investico (a platform for investigative journalism) for the Dutch newspapers Trouw and De Groene Amsterdammer shows that the driving force behind smart city projects in the Netherlands is often not the municipality, but industry.⁸ That research showed that Dutch municipalities do not always have access to the data that is collected by the companies that deliver these smart services.⁹ For example, the Dutch company CityTec – that manages 500,000 smart city lights, 30,000 traffic lights and 2,000 parking installations – states that it does not want to share its data with the municipalities, in order to protect its market position.¹⁰

As mentioned before, smart city lights can be equipped with wifi trackers, a system that receives and follows the signal of the wifi from a smartphone. By tracing the signals of phones, the company that installed the wifi tracker can follow and analyse flows of people and could potentially also trace the data to an individual. An increasing number of shops use wifi trackers to identify the shopping behaviour of their customers, without the consent or even knowledge of

5 Seubers, A. (2018). Nederland als smart city-exportland. Available online at: <https://www.computable.nl/artikel/expertverslag/overheid/6400397/4573232/nederland-als-smart-city-exportland.html>.

6 Idem.

7 NL Smart City Strategie: The future of living (2017, 25 January). Available online at: https://www.thehaguesecuritydelta.com/media/com_hsd/report/114/document/NL-Smart-City-Strategie-.pdf.

8 Teeffelen, C. & Naafs, S. (2017, 5 December). Moeten we wel zo blij zijn met de slimme stad? In: Trouw. Available online: <https://www.trouw.nl/nieuws/moeten-we-wel-zo-blij-zijn-met-de-slimme-stad-baa1a488/>.

9 Teeffelen, C. & Naafs, S. (2017, 5 December). Moeten we wel zo blij zijn met de slimme stad? In: Trouw. Available online: <https://www.trouw.nl/nieuws/moeten-we-wel-zo-blij-zijn-met-de-slimme-stad-baa1a488/>.

10 Naafs, S. (2017, 6 December). De muren hebben sensoren. In: De Groene Amsterdammer. Available online at: <https://www.groene.nl/artikel/de-muren-hebben-sensoren>.

their customers. The European General Data Protection Regulation (GDPR), which came into force in May 2018, does not allow the use of wifi trackers. However, a study by the Dutch newspaper De Volkskrant found that the two main suppliers of wifi trackers in the Netherlands were still supplying wifi trackers to at least 60 Dutch municipalities (including Amsterdam and Rotterdam) around the end of May 2019.¹¹ In other words, it seems that government control of the use of smart technologies in Dutch cities is currently inadequate.

According to Professor Pras from Twente University nobody knows exactly which data are collected in smart city projects and with what aim.¹² It is about time that we mapped the companies in the Netherlands that collect privacy-sensitive data and introduced clear legislation for the storage, analysis and selling of this data, before continuing the smart city developments.

The two large wifi-tracking companies in the Netherlands are Dutch. However, where do they store their data? More than half of all Dutch companies have shifted their services to servers in data centres outside of their organizations.¹³ The study by Smart Profile shows that in the Netherlands government and health organizations are those that most often outsource their servers: 70% and 71% per cent respectively. The most popular cloud service hardware suppliers in the Netherlands are from the U.S.: HPE (54.5%), DELL EMC (30.5%) and Cisco (5.9%).¹⁴ And the most popular service providers are

also from the U.S.: Amazon, Microsoft and Google. It is important to know where these U.S. companies store the Dutch data and who owns the data because it determines how much control the Dutch government has to protect the privacy and safety of its citizens.

The Patriot Act signed into law on 26 October 2001 by President George W. Bush requires U.S. providers to give the U.S. government access to data that is stored in their data centres abroad. However, in a court case against Microsoft in 2013, the U.S. government realized that the legislation in place did not allow the U.S. government to gain access to data stored by U.S. companies abroad.¹⁵

In 2013, the U.S. government argued that the Microsoft data stored in Ireland fell under the Stored Communications Act. Microsoft disagreed with the U.S. government and filed a lawsuit. Microsoft won and the U.S. Department of Justice filed an appeal with the Supreme Court. However, the U.S. government did not wait for the decision from the Supreme Court and adopted the CLOUD Act instead. The CLOUD Act removes the right of U.S. companies to challenge a judicial ruling to share their stored data in Europe. On the other hand, the European GDPR protects the transfer of personal data outside the EU and European Economic Area. In other words, there is no clarity yet concerning the ownership and control of data collected by U.S. companies in Europe that is stored in Europe.

Meanwhile, Chinese firms are catching up with U.S. firms: Alibaba, Tencent and Baidu have become serious competitors for U.S. cloud providers and Huawei and Lenovo have become serious competitors for U.S. cloud hardware suppliers. Could we expect data leaks to China through smart cities in the near future?

11 Verhagen, L. (2019, 31 May). Tientallen Nederlandse gemeenten volgen u met wifitracking. Available online at: <https://www.volkskrant.nl/nieuws-achtergrond/tientallen-nederlandse-gemeenten-volgen-u-met-wifitracking~b5c614ad/>.

12 Naafs, S. (2017, 6 December). De muren hebben sensoren. In: De Groene Amsterdammer. Available online at: <https://www.groene.nl/artikel/de-muren-hebben-sensoren>.

13 Smart Profile (2019, 23 July). Smart Profile: HPE blijft server markt aanvoeren. Available online at: <https://dutchitchannel.nl/627756/smart-profile-organisaties-kiezen-vaker-voor-externe-servers.html>.

14 Idem.

15 Hurley, L. & Volz, D. (2018, 27 February). U.S. Supreme Court wrestles with Microsoft data privacy fight. In: Reuters. Available online at: <https://www.reuters.com/article/us-usa-court-microsoft/u-s-supreme-court-wrestles-with-microsoft-data-privacy-fight-idUSKCN1GB0GY>.

China is becoming a high-tech leader

In May 2015 the Chinese Premier Li Keqiang issued 'Made in China 2025', a strategic plan to upgrade Chinese industry. The aim of this upgrade is to fully integrate China in the high end of the global production chain. The leading principles are: innovation-driven, emphasis on quality rather than quantity, sustainable economic development, improving the structure of Chinese industry and nurturing human capital. Whereas previously the focus was on catching up in whatever way possible (accepting the dirty heavy industry of other countries and copying its way up the ladder), China is now ready for the next step of becoming more like the advanced markets, with a focus on high-end technology and employee satisfaction.

In July 2017 China's State Council launched a ground-breaking document that presented the Chinese attitude toward artificial intelligence and its applications: the Artificial Intelligence Development Plan (AIDP). This document argues that the rapid developments in AI will radically change society, life and the world; and China wants to be a frontrunner in the area of AI. The Chinese government aims to achieve that goal in three stages:

1. In 2020 Chinese AI technology and its applications will be at the same level as the technology of the advanced companies in the West.
2. In 2025 some Chinese AI technologies will be among the world leaders and AI will be the most important driving force of the economic transformation in China.
3. In 2030 China will be the world's primary AI innovation centre.

One of the driving forces behind the AIDP is the dependence of Chinese tech firms on foreign-produced chips. For the past two decades Huawei alone has paid more than US\$ 6 billion on fees and royalties, with nearly 80% of that amount paid to

US companies.¹⁶ China is tired of paying big sums for royalties and licence fees to Western firms. Western countries might have a trade deficit with China, but China has a huge intellectual property deficit: in 2017 Chinese firms received US\$ 1 billion from foreign companies, but paid almost US\$ 20 billion in royalties and licence fees.¹⁷

Although a latecomer to the AI industry, China is quickly closing the gap with its structural advantages: the scale of its market, the centrally organized government and Party, the absence of privacy laws and regulations, and its collaborative approach by using the strengths of its top technology companies.

A good example of China's collaborative approach is the cooperation between Ping An, Alibaba, Tencent and Huawei, which jointly developed a smart cities initiative for China known as the 'PATH to Smart Cities'. The possibilities are enormous when these giants pull their resources together. Ping An (P) is the largest insurance company in the world. Since 2008 it has invested 10% of its profit every year in new technologies such as AI, blockchain and Cloud Computing.¹⁸ So far Ping An has invested about RMB 50 billion (around €6 billion) in technology research and aims to invest another RMB 50 billion in the next 10 years.¹⁹ It employs

16 Huawei (2019, 27 June). Respecting and Protecting Intellectual Property: The Foundation of Innovation. Huawei White Paper on Innovation and Intellectual Property. Available online at: https://www-file.huawei.com/-/media/CORPORATE/PDF/white%20paper/2019/Huawei_White_Paper_on_Innovation_and_Intellectual_Property.pdf.

17 Dodwell, D. (2017, 24 March). Be afraid: China is on the path to global technology dominance. In: South China Morning Post. Available online at: <https://www.scmp.com/business/global-economy/article/2081771/be-afraid-china-path-global-technology-dominance>.

18 Chen, S-C. J. (2018, 6 June). Chinese Giant Ping An Looks Beyond Insurance To A Fintech Future. *Forbes*. Available online at: <https://www.forbes.com/sites/shuchingjeanchen/2018/06/06/chinese-giant-ping-an-looks-beyond-insurance-to-a-fintech-future/#40be012648f3>.

19 Ping An Technology (2018). <https://tech.pingan.com/en/>.

about 30,000 R&D professionals and more than 500 big data scientists who are exploring several technology areas including AI, blockchain, fintech and health-tech.²⁰ For the 'PATH to Smart Cities' initiative Ping An provides the cloud platform that supports the various smart elements of a city.

Other PATH members bring their own unique strengths. Alibaba (A) enables smart retail through AliPay, offers cloud services via Alibaba Cloud and its City Brain improves the mobility in cities with the help of AI.²¹ Tencent (T) helps residents stay connected with each other and with businesses on China's largest social media platform, named WeChat. Huawei (H) provides core hardware technology with smartphones, telecom infrastructure, maritime internet cables and cloud supplier services. In other words, China has become largely self-sufficient with regard to smart city technology. At this moment, China only relies on foreign-produced chips and chip-making machines.

The Netherlands is more dependent on Chinese and other foreign technology. Huawei is the world's leading telecom infrastructure company. It is therefore not surprising that the Dutch telecom company KPN uses Huawei equipment in its core network.²² The safety of the use of Huawei hardware (in terms of espionage) has recently been intensively debated, especially in the run-up to the introduction of 5G networks. However, the European alternatives Ericsson and Nokia produce many parts of their networks in China and are therefore not necessarily a safer alternative. There are more of these less visible connections between Chinese and

Western companies that could potentially lead to more hidden data leaks.

Possible data leaks: existing entanglements with Chinese firms

It requires a more extensive study to gain a full picture of the presence of Chinese firms in the Dutch smart city market and the ways in which Dutch data could possibly leak to Beijing. However, a quick scan can give us some insight into the importance of such a study.

Take, for example, the E-gate at Schiphol. This is a technology developed by Vision-Box and Accenture that enables travellers to check in by themselves using facial recognition technology.²³ Accenture is a U.S.-based company and one may wonder whether a non-European company should have access to and control of such personal data. It becomes more complicated, however, because Accenture has strategic alliances with Alibaba Cloud²⁴ and Shenzhen-based Malong technologies.²⁵ What impact do these alliances have on the flow of the data gathered by Accenture at Schiphol?

20 Ping An Insurance Group (2018). Smarter life, better future: Sustainability report 2018. Available online at: http://www.pingan.cn/app_upload/file/official/2018ESGReport_EN.pdf.

21 Toh, M. & Erasmus, L. (2019, 15 January). Alibaba's 'City Brain' is slashing congestion in its hometown. In: CNN. Available online at: <https://edition.cnn.com/2019/01/15/tech/alibaba-city-brain-hangzhou/index.html>.

22 Pelgrim, C. (2019, 26 April). KPN weert Huawei een beetje. In: NRC. Available online at: <https://www.nrc.nl/nieuws/2019/04/26/kpn-weert-huawei-een-beetje-a3958332>.

23 Accenture (2016, 26 November). Automated Border Clearance at Schiphol Airport: Interview with Kier-co Gerritsen, Program Manager. Available online at: https://www.accenture.com/t20161123t000738_w_gb-en_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/industries_8/accenture-automated-border-clearance-at-schiphol-airport-interview-with-kier-co-gerritsen.pdf.

24 Alibaba Cloud (2016, 20 April). Alibaba Cloud Announces Collaboration with Accenture to Deliver Cloud Services and "As-a-Service" Solutions to Clients in China and ASEAN Markets. Online available at: <https://www.alibabacloud.com/press-room/alibaba-cloud-announces-collaboration-with-accenture-to-deliver-cloud>.

25 Soh, P., Han, I. Y., Kutz, K. and Peng, P. (2018, 13 August). Accenture Forms Strategic Alliance, Invests in Chinese AI Start-up Malong Technologies. Online available at: <https://www.businesswire.com/news/home/20180812005014/en/Accenture-Forms-Strategic-Alliance-Invests-Chinese-AI>.

There are many more examples of such entanglements between Western and Chinese firms. For example, some U.S. camera manufacturers use Huawei's HiSilicon in their security cameras. We might consciously decide not to use Chinese Hikvision cameras to secure premises in the Netherlands; however, what do we know about the origin of the parts in cameras from non-Chinese brands? What, for instance, are the consequences of the cooperation between Deloitte and the Chinese AI company SenseTime for those Dutch companies that make use of Deloitte's recently advertised AI services? What are the consequences for the data from Dutch companies that is stored with Microsoft Azure, OneDrive or IBM Cloud since Microsoft and IBM cooperate with the large Chinese cloud computing company Inspur? Where is the data that Alibaba, WeChat Pay and Accenture collect at Schiphol stored? The fact that there are no ready answers to these questions shows the urgent need for more research on this topic.

City managers who aim to develop their city into a smart city should start with a smart strategy for how to control the infrastructure and store and manage the data that is collected in their cities. Otherwise Dutch cities risk becoming dumb cities: cities that give free rein to (foreign state-owned and) private companies to spy on their citizens with all the potential security and privacy risks while missing out on the opportunity to actually improve the services for their residents.

Conclusion





In theory, rules such as the EU law on data protection and privacy (GDPR) should constrain Chinese businesses from sending personal data collected in the EU to China. However, the case of the U.S. CLOUD act shows that the international regulations for data protection are anything but clear. Therefore it is necessary to map the links between Western and Chinese companies in order to increase our understanding of the potential risks of data leakage and to devise measures to protect ourselves against these risks. Furthermore, it is important for the Netherlands and the EU to keep investing in new-generation technologies in order to catch up where Europe lags behind. In this regard it is hopeful that the President of the European Commission, Ursula von der Leyen, has given Margrethe Vestager the task of developing a European AI strategy in the first 100 days of her mandate.²⁶

26 Leyen, von der, U. (2019, 10 September). Margrethe Vestager: Executive Vice-President-designate for a Europe fit for the Digital Age. Mission Letter. Online available at: https://ec.europa.eu/commission/sites/beta-political/files/mission-letter-margrethe-vestager_2019_en.pdf.

About the Clingendael Institute

Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

 @clingendaelorg
 The Clingendael Institute
 The Clingendael Institute
 Newsletter

About the author

Sanne van der Lugt joined Clingendael in 2019 as an Associate Fellow. Her research is aimed at the consequences of China's re-emergence as a global power for Europe, with a special focus on China's economic activities in Africa and China's position in the fourth industrial revolution.