

Kajander, Aleks; Hoffmann, Thomas

Article

Smart city data commons and EU competition law: A conflict in the making?

Scientific Papers of the University of Pardubice, Series D: Faculty of Economics and Administration

Provided in Cooperation with:

Faculty of Economics and Administration, University of Pardubice

Suggested Citation: Kajander, Aleks; Hoffmann, Thomas (2024) : Smart city data commons and EU competition law: A conflict in the making?, Scientific Papers of the University of Pardubice, Series D: Faculty of Economics and Administration, ISSN 1804-8048, University of Pardubice, Pardubice, Vol. 32, Iss. 2, pp. 1-10,
<https://doi.org/10.46585/sp32022092>

This Version is available at:

<https://hdl.handle.net/10419/334836>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<https://creativecommons.org/licenses/by/4.0/>

Smart City Data Commons and EU Competition Law – A Conflict in the Making?

Scientific Papers of the University of Pardubice, Series D: Faculty of Economics and Administration 2024, 32(2), 2092.
©The Author(s) 2024. This is an open access article under the CC-BY 4.0 license.
DOI: 10.46585/sp32022092
editorial.upce.cz/SciPap

Aleksi Kajander 

Tallinn University of Technology, Department of Law, School of Business and Governance, Estonia

Thomas Hoffmann 

Tallinn University of Technology, Department of Law, School of Business and Governance, Estonia

Abstract

Open data has been heralded as bringing great benefits to businesses and individuals alike in the EU, enabling the emergence of a data agile Europe and a society empowered by data. However, such arrangements are far from being free of disadvantages, especially for the citizens of smart cities. If the data generated by smart cities is made open almost by default, there is a serious risk of data disenfranchisement for the smart citizens, who may be negatively impacted by the publication of even non-personal smart city data. Consequently, Ostrom's commons have been considered as a possibility to re-empower smart citizens in regard to their data through self-governance. However, should smart citizens decide to make data available only to select users, they could potentially run into a conflict with EU competition law. Potential sources of conflict include violations of Articles 101 and 102 of the TFEU, through decisions made in the context of the self-governing smart city data commons. Consequently, this paper seeks to identify the potential conflicts between managing non-personal smart city data as a commons and EU competition law.

Keywords

Smart city, Data, Commons, Ostrom, Competition law, European Union,

JEL Classification

K21, L86, O34, R38, D86, H83

Introduction

The EU's 'European strategy for data' contains a vision for the future, where the availability of data enables both the private and public sector to make better decisions largely through open data (European Commission, 2020), for the availability of data is the 'lifeblood' of the hoped for economic development, and as such the EU's legal framework has already been transformed to meet this vision (European Commission, 2020, p. 4). Examples of this include the General Data Protection Regulation (GDPR) intended to build digital trust, as well as legislation aimed at the availability of data, such as most recently the 2022 Data Governance Act, the 2018 Regulation of the free flow of non-personal data (FFD) and the Open Data Directive. Furthermore, competition law is set to play an important role in the transformation, as the strategy noted the need to examine the competition law effects of large-scale data accumulation and data-access or sharing remedies (European Commission, 2020, p. 14).

This latter development is primarily aimed at Big Tech companies, as noted in the strategy itself, which accumulate and own vast amounts of data and as such hold considerable bargaining power (European Commission, 2020, p. 14). Indeed, against this development, the focus on open data appears to be the logical solution, for if data availability is maximized, it should enable competitors to enter the market and reduce the bargaining power of the 'Big Tech' companies, thereby reducing the distortion to the market. However, underneath the considerations for the data accumulation of 'Big Tech' and the drive for open data lies the risk of ignoring the effects which open data policies may have on the individual citizen, especially those who reside in smart cities.

While many smart city definitions exist, arguably a common underlying thread is that any city can be considered a smart city as far as it incorporates information communication technologies to collect and communicate data that is used to improve its efficiency and competitiveness (Zofcinova, Cajkova, and Kral, 2022, p.10). Consequently, the individual smart citizen (Fernández-Montesinos, 2020) inhabiting such a city will generate a considerable amount of data that will be captured by the surrounding sensors, which will either trigger legal transactions (for instance in form of oracles within smart contracts, Hoffmann, 2019, p. 168) or be collected for yet undisclosed purposes – but either way it will have considerable commercial value. However, often the smart citizen is reduced to the role of a consumer within a marketplace with little opportunity to step outside their intended role and actively

Corresponding author:

Aleksi Kajander, Akadeemia tee 3, 12611, Tallinn, Estonia
Email: aleksi.kajander@taltech.ee

participate in for example the management of the data (Knieps, 2017, p. 825).

This type of smart city model can be called the 'neoliberal' or 'corporate-led' model, which arguably describes the EU strategy for data. Even though this strategy refers to transparency, protection and oversight of personal data in various contexts, its main objective is fostering businesses and economic benefits generated from the availability of data (European Commission, 2020, pp. 4-5). This also implies individual rights given to citizens, which are viewed through the lens of competition benefits (Ibid, 2020, p. 10). Notably absent from the strategy are any collective rights for smart citizen to be able to decide what is done by the non-personal data that they generate.

As a counterbalance to the 'corporate-led' smart city model, the 'sustainable smart city' or 'humane smart city' models suggest emphasizing and empower the role of the individual smart citizen (Kajander, 2022, pp. 10-11). As a part of these alternative models, the incorporation of data as "commons" in terms of Ostrom's theory (Ostrom, 1990, p. 188) has been suggested to provide a true alternative to data management through private businesses or public institutions by the incorporation of self-governance (Lange, 2019, p.11). Knowledge commons have been defined as the common arrangements intended to overcome the social dilemmas arising from the sharing and producing of information (Marques et al, 2021, p. 11). While it is apparent that personal data can result in social dilemmas, it is already extensively governed by the General Data Protection Regulation (GDPR) in the EU, and as such citizens are already empowered regarding it. However, EU citizens arguably have negligible control over non-personal data. As non-personal smart city data nevertheless can impact the lives of smart citizens considerably, not to mention create social dilemmas, knowledge commons are arguably a fitting potential solution to its management and as such will be the focus of this paper.

However, with such self-governance arises the possibility that the data may not be made available for all, which could bring such ideas for data commons to a conflict with the EU legal framework. A decision to not share smart city data with certain entities that is made by a smart citizen common could put them in breach of EU competition law - for example of Article 102 (c) TFEU by applying dissimilar conditions to equivalent transactions. While this premise may sound initially far-fetched, as many of the more readily identified competition concerns surround the 'Big Tech' companies and their dominance of the market, the market power of smart city data commons (SCDC) could be considerable in the future. Their data governance actions could thus plausibly attract competition law attention, which may amount to an obstacle for the introduction or development of such citizen governance within the framework of EU competition law. This paper therefore aims to identify the potential conflicts between SCDC for non-personal data and EU competition law. Furthermore, the paper intends to outline the implications of this potential conflict with competition law on the possibility of introducing commons-orientated smart city data governance in the EU.

Literature Review

Non-Personal Smart City Data and the Need for Commons

The EU's strategy for data is centered around the availability of data which promises to be the 'lifeblood of economic development' enabling improved productivity and resource efficiency (European Commission, 2020). The strategy goes as far as to state that data is an 'essential resource' for start-ups and small and medium-sized enterprises (Ibid, 2020). Consequently, the free movement and sharing of data is essential for the vision of the EU for a 'data-agile' economy. However, that data must be obtained from somewhere, one such place being (future) smart cities' data sharing infrastructures, which produce and share an abundance of both personal and non-personal data through their sensors.

This smart city data, which can be defined as data generated and derived from the ICT infrastructure that constitutes a smart city (D'Ignazio et al, 2019, p. 133), will largely be created by the action and behaviour of individual smart city's residents. The abovementioned EU vision for data arguably assumes the smart citizens' consent to share all the data they generate whilst inhabiting a smart city as a forgone conclusion. This is reminiscent of the criticism of the 'neoliberal' model for smart cities where the citizens are passive data providers that form the 'raw material for algorithms that can be turned into commodities (Calzada, 2018, p. 6).

This highlights an important overshadowed aspect of the transformation to a single European data space and the data agile economy - the role, conditions, and willingness of the citizens to function as data donors. While it is not entirely fair to state that the citizens' perspective is not addressed in the EU's strategy for data, arguably it amounts to lip service to the idea of actually empowering smart citizens. This is demonstrated by the EU's own vision in 'empowering' citizens which has a twofold focus - data mobility to foster competition and protection of privacy.

The first point is exemplified by the focus on Article 20 of the GDPR in the strategy which provides consumers the ability to change service providers easier by migrating their data, and thereby 'fostering competition'. Secondly, even the privacy concerns are primarily cantered around economic benefits from better service and management of one's own data in the personal data economy (European Commission, 2020, p. 10). What is absent from both these concerns is the collective ability of smart citizens to decide what happens to the data that they generate by inhabiting a smart city. Arguably, the vision for 'empowering' citizens in the EU's strategy for data is in line with the

'neoliberal' smart city vision of a consumer with a tokenistic ability to manage their personal data. The collective management of non-personal data by smart citizens is not a consideration in the EU's strategy for data, instead there is a presumption that such data should be automatically shared in accordance with the Open Data Directive and the Free Flow of Non-Personal Data Regulation. Consequently, the ability of citizens to collectively oppose the sharing of certain non-personal data sets is arguably limited to non-existent.

Nevertheless, in the EU legal framework, it may be argued that there is no need for citizens to be able to govern their non-personal data, as they are adequately protected by the GDPR. This impression can, however, be deceiving, despite the GDPR extending protection to 'any information relating to an identified or identifiable natural person', which would seem to imply that if the data has any bearing on an individual directly, that individual will have control over it. Indeed, the scope is so broad that there have been arguments that it is too wide, and that essentially all data could amount to personal data in certain contexts - including the weather (Purtova, 2018, pp. 2-3). This argument was somewhat strengthened by the Breyer case where the CJEU found that personal data includes data, which by itself does not identify a person, but if additional data can lawfully be acquired that will identify the individual, then the initial data where the subject is not identified could be considered personal data, at least for dynamic IP addresses (El Khoury, 2018, p. 170). This in turn could be argued to extend the scope of the GDPR as it could, in theory, transform initially seemingly non-personal data to personal data based on the future availability or existence of additional information that would make the data relate to an identifiable individual. Nevertheless, until the CJEU confirms this argument regarding the scope of the GDPR, it cannot be truly relied upon, and as such this paper will use the conventional approach to personal data, whereby data that does not indirectly or directly relate to an identifiable person will be considered non-personal.

However, it is evident that non-personal data is not free of consequences, even though it does not directly relate to any identified or identifiable person, and therefore there exists a need for individuals to be able to govern its dissemination. An example of this is case study by Beckwith et al on the commons created to manage flooding data by local residents (Beckwith, Sherry and Prendergast, 2019). The residents felt that a full release of the data could result in potentially unjustified consequences for the homeowners in the area, and as such opted for a strategy of limited dissemination (Ibid, 2019). Under the current interpretation of the GDPR, the flooding data would be classified as non-personal data as it does not relate to any identified or identifiable person.

Nevertheless, as demonstrated by the residents' concerns, its disclosure could have significant implications for them. Furthermore, it is evident that the data would need to be managed collectively by the affected community, as the data will not impact only those who collect it, but everyone in its proximity, for even if one resident does not record data but their neighbours do, the implications of the data would extend to those who 'opted out' of collecting the data. Moreover, these effects may not be felt immediately, but for example only when an individual attempts to sell their house, whereby the data would hang above them like a modern sword of Damocles, having the potential to fall on the residents and impacting them negatively during future circumstances. Consequently, there is arguably a clear and convincing case for non-personal data to be managed collectively by those affected by it, which in the case of a smart city would be its citizens.

Moreover, this necessity is arguably heightened in the case of a smart city, which increases the number of data points that can be recorded (Madison, Sanfilippo, Frischmann, 2023, p. 12). Therefore, unlike in the flood data example, there is not just the impacts of releasing one type of data to consider, but the collective effect of multiple different types of data. It is logical that as even one type of data can result in social imbalances, then multiple types of different data are almost certain to result in greater and more numerous social dilemmas. The case of real-time open traffic data through Waze demonstrated the emergence of various social dilemmas, such as the efficiency of traffic versus the safety and comfort of residential areas (CBS News, 2014). The residents of affected areas lacked the means to control the conditions for sharing such data, which a knowledge common as the common arrangements intended to overcome the various social dilemmas that result from the sharing and producing of data (Marques et al, 2021, p.11), would provide for the area. Therefore, the governance of non-personal smart city data as a knowledge common is not only an appropriate solution, but a necessity.

The above example demonstrates several key points. Firstly, non-personal data has the power to impact the lives of individuals considerably. Secondly, smart city non-personal data may be undesirable to be made public, especially in real-time, owing to its power to impact citizens. Therefore, non-personal data has the ability hang like a modern sword of Damocles over the residents of an area, whereby its impact may be felt immediately such as with Waze's real-time traffic data or it may be felt further in the future as the residents in the flood plain example feared. Consequently, smart citizens have a legitimate reason to be able to govern the release of such 'data of Damocles'.

Hence, there is a situation that calls for the smart citizens to be able to govern the data they generate in the context of a smart city. In this respect, Ostrom's commons have been suggested as a possible solution to this governance conundrum, especially as the commons framework is well-suited to data (Raymond and Kouper, 2023, p. 58). The commons represent an alternative to either private or public governance of a resource that is subject to social dilemmas (Marques et al, 2021, p. 11). As noted above, even non-personal data is subject to social dilemmas as

it may hang over the populace like a modern sword of Damocles, whereby arguably there is a necessity for the community to decide to which extent are they willing to accept such risks from the sharing of data. Furthermore, experience has already demonstrated that public authorities are often incapable of resisting the private sector's offers for providing smart city infrastructure in exchange for the data (Morozov and Bria, 2018, p. 18), which disenfranchises the citizens. Consequently, it is arguably necessary to empower citizens, in regard to not only their personal data, but additionally their non-personal data, which can be achieved through the incorporation of SCDCs that are self-governed and able to decide the conditions for sharing the data generated by their smart city.

Methodology

A smart city data commons (SCDC) is unlikely to attract any competition law controversy as long as it follows an 'open data' policy, whereby the data is made available equally to all interested parties. However, the purpose of a commons is the self-governance of the resource, the value of which lies in the ability to make meaningful choices, including making it available only to certain users. Hence, for a SCDC to be meaningful, it must be able to deny access to the valuable smart city data.

However, as the commons would be the sole gatekeeper to the data, conceivably, at least *prima facie*, its decisions could, in some cases, potentially be characterized as an abuse of dominant position under Article 102, as the commons effectively holds a data monopoly. Consequently, this paper will use existing caselaw to determine whether it is likely that SCDC could fall afoul of Articles 101 and 102 of the TFEU.

The Legal Form of Smart City Commons

Before either TFEU article can be discussed, the practical question of what legal form would a SCDC actually take has to be addressed. The importance of this question lies in establishing whether a SCDC as an entity would even be within the scope of EU competition law. The provisions of EU competition law are targeted towards 'undertakings'. This is demonstrated succinctly by Article 102 of the TFEU, whereby the provision applies to 'undertakings', that are in a 'dominant position' which has the capacity to 'affect trade between Member States'. Consequently, for SCDC to be in the scope of EU competition law, firstly they must be an 'undertaking'. Secondly, whether they are captured by Article 102 will depend on whether they can be characterized as being dominant and if it is a potential effect on the trade between Member States. Similarly, Article 101 applies to 'undertakings' or 'associations', hence, for an entity to be in the scope of EU competition law it must be an undertaking.

The forms of 'traditional' commons that Ostrom originally studied, such as the collection of fishermen families in Alanya, Turkey were rather informal from a legal point of view, with the management of the fishing grounds being best described as a collection of agreed rules among the small number of fishers absent any particular legal form (Ostrom, 1990, p. 188). The commons in Valencia did employ a pseudo-court without lawyers to settle water disputes for the autonomous irrigation communities (Ibid, p. 71), however, these structures are far from the legal forms that one would encounter in a business register. However, in the more formal environment of a city, such informal collectives will not be viable, especially if they are to be vested with the ability to govern data, and therefore arguably they must have a defined legal form. Commons in urban settings have already taken the form of not-for-profit associations (Balestrini et al, 2017, p. 2288), and trusts (Chyi and Wu, 2023, pp. 85-86), whereby depending on the national laws the exact legal form may vary based on the available national options. However, it is evident that a SCDC must have some legal personality and be registered in some form, be it as a trust or a not-for-profit association.

Hence, while the exact legal form a SCDC may vary country to country, the scope of EU competition law is arguably broad enough to encompass all the variations. As the term "undertaking" itself is not defined within the TFEU, the case law of the Court of Justice of the European Union is used to define the term (Okeoghene, 2005, p. 213). In the judgement in *Höfner*, 'every entity engaged in economic activity, regardless of the legal status of the entity and the way it is financed' is considered an undertaking under EU competition law. Hence, it is irrelevant what legal form the entity takes, that is to say, a private company, a not-for-profit association, or something else in terms of determining whether the entity is covered by EU competition law. Furthermore, its source of financing is irrelevant, rather what is important is whether it engages in 'economic activity', which as the subsequent caselaw has demonstrated, can be occasionally difficult to define (Van der Gronden, 2018, p. 199).

'Economic activity' is defined by the CJEU as 'the offering of goods and services on the market', which while concise is somewhat unhelpful as it is effectively circular owing to the use of the term 'market' which is essential identical to the term 'economic' (Ibid, 2018). The CJEU has further considered that an essential part of 'economic activity' is competition, i.e. that even if there is no seeking of profit but the providers of the good or service are in competition with each other, the activity is to be considered economic (Ibid, 2018, p.200). This is arguably somewhat problematic in the commons context, as in the case of *MOTOE* the Court considered that even if motorcycle competitions did not seek to make a profit, their survival depended on outperforming their competitors. This raises a potential problem in the commons context, if the survival of a community association intended to self-govern data is dependent on any form of success to survive. While it is difficult to argue in the abstract conclusively either way,

doubts could be raised as to whether a community would stop collectively self-governing their data if they are 'outperformed' by other SCDCs, or if their commons was not generating income. Alternatively, it could be argued that if a SCDC does not share its data competitively compared to other commons, it will be a less desirable location for businesses, which in turn will reduce tax revenues, employment opportunities, and ultimately the standard of living, whereby it is in the commons' interest to be 'competitive'. Therefore, it is not inconceivable that the economic activity criteria would be fulfilled by a SCDC.

Another significant issue in the application of competition law is the definition of the (data) market. CJEU case law has established that 'hypothetical competition' is sufficient, which is to say that a service 'could be supplied in competition on the marketplace' for that to activity to be considered economic in nature (Sauter and Schepel, 2010, p. 82). The data 'market' for smart city data may be characterized in various ways. Firstly, it is necessary to recognize that a SCDC is most likely to be defined by a geographical scope, i.e. it will include the natural persons residing in the area covered by the smart city's sensors. Consequently, the commons would be able to determine the governance of the data in that geographical area, which is to say, they would essentially have a natural data monopoly over the city they self-govern.

Therefore, in a narrow definition of a data market, that of the city itself, there cannot be any competition on the market as there are no alternatives, at least for the data generated through the smart city sensors the commons governs. Consequently, any downstream market products that are dependent on such data will be entirely at the mercy of the commons' decisions as they effectively hold a natural monopoly and therefore depend on it for data access. In this regard, there would be no competition on the market, and as such the commons' would not have to compete for survival.

However, if the market scope is broader, that is to say for example the data market of a specific country that encompasses many separate SCDCs, such as in the case where each city would have a commons, then it could be argued that the commons is competing with other commons. Similarly, there could even be intra-smart city competition if different blocks of the city are governed by separate commons. Thus, it could be argued that the commons are competing among each other, for if data is the 'lifeblood' of the economy, then those smart cities that are most willing to share the data will also attract the most businesses, which in turn ensures their survival. This in turn incentivizes competitive behavior in offering the smart city data, as not doing so could compromise the future of the commons and the area it covers.

This will naturally scale up if examined on an EU-level, where the data sharing practices of different EU MS will similarly impact the economic success of the Member States. The larger definition for a data market and the ambition for a single market for data contained in the EU strategy on data would appear to be the most likely focus taken by the CJEU, especially as there is a requirement that the trade between MS could be affected for EU competition law to apply. Hence, it is clearly not inconceivable that the activities of the commons could be classified as fitting the concept of 'economic activity', and as such would be within the scope of EU competition law. Naturally, it will be for the CJEU to make a final determination, however, based on the existing case law and the concept of the SCDC, it seems reasonably possible that such commons would be in the scope of competition law.

Consequently, it is evident that there is a reasonable possibility that SCDCs would be within the scope of competition law, and as such may be subject to conflicts with the EU's competition law framework. Considering the natural monopoly like position and absence of substitutes, violations of both Article 101 and 102 of the TFEU are entirely plausible.

Results

Violations of Article 101 TFEU

The possibility of self-governance by a commons of smart citizens in a smart city brings with it plausible scenarios under which a commons or group of commons could violate EU competition law. As was established above, a SCDC can be considered an undertaking in the EU competition law sense, whereby the actions of a commons are within the scope of competition law. Consequently, attention must be turned towards the plausible scenarios in which violations of Article 101 of the TFEU could occur from decisions made by a commons regarding the sharing of their smart city data.

It is not inconceivable that a SCDC for one city would pool their data with another city, in order to improve its value, by creating a larger common pool of data. This could very well take place across EU Member State borders, such as in the context of the proposed FinEst Twins which seeks to create a cross-border smart city centre of excellence between Tallinn and Helsinki (Soe, 2022, p.3). As noted earlier, for EU competition law to be relevant, the infringement must have the potential to affect trade between Member States, whereby a cross-border smart city commons' decisions would definitely qualify. In the context of Article 101 TFEU decisions by commons that pool data together and agree to common conditions for the sharing or selling would be relevant. Such decisions could at least *prima facie* be considered to be agreements between undertakings that may restrict or distort competition within the internal market, in the meaning of Article 101 TFEU.

However, it is worth noting the purpose behind Article 101. As stated in the Guidelines for Vertical Agreements for Article 101 TFEU, Article 101 is to protect the consumers from agreements between undertakings, vertical or horizontal, that distort competition to the detriment of consumers. As a smart city commons would be constituted from the natural persons who live within the smart city and thereby generate the data and collectively self-govern via the commons, therefore it is largely, if not entirely, governed by consumers. Although it must be noted that EU competition law, unlike consumer protection law, equates customers to consumers, which includes businesses in addition to natural persons, in order to avoid a cumbersome process to trace every competition law breach's effect to the final natural person level (Robertson, 2018, p. 40). Nevertheless, arguably the ultimate object of protection is the same i.e., natural persons.

Consequently, it is a perplexing notion that decisions taken by what is essentially an association of residents (being data generators and consumers simultaneously) may be subject to legal control through competition law in order to protect themselves from the detriment of their own decisions. This is particularly fascinating as considering that arguably the majority of the potentially detrimental competition effects would be felt within the geographical area of the commons itself. For if data is not made available to improve the efficiency of businesses within the smart city, the effects will be primarily felt by the residents of that city rather than other consumers residing outside the commons. Similarly, the overruling of the commons' decisions could arguably be detrimental to local 'consumer welfare' whereby it would be contrary to the principles of competition law.

However, currently, based on the notion and treatment of 'green antitrust' (Volkovski, 2022, p. 512), it does not seem likely that SCDCs would receive special treatment. 'Green antitrust' refers to the notion that measures that might otherwise be in violation of competition law, such as cooperation prohibited by Article 101, could either be exempt or receive special treatment due to their objective of achieving sustainability (Ibid, 2022, p. 502). In terms of national law, the Austrian Cartel Act was amended in 2019 to include a provision that carved out the 'world's-first green exemption' may be held as an example of 'green antitrust' (Zelger, 2022, p. 515). However, in the 2022 Guidelines on Vertical Agreements, the Commission explicitly states that such vertical agreements which pursue sustainability or 'contribute to a digital and resilient Single Market' are in fact, 'not a distinct category of vertical agreements', and as such are subject to the same conditions as all non-sustainable agreements. It is worth noting the reference to vertical agreements that 'contribute to a digital and resilient Single Market', would not receive special treatment either, implying SCDC are equally unlikely to receive special treatment.

Furthermore, SCDC would likely fragment the digital single market rather than contribute to it. For unlike the EU's vision of sharing non-personal data, the self-governance data through commons, could fragment the data market through differing conditions for sharing data imposed by each commons. Hence, there would arguably be even less incentive, from the EU's perspective, to grant favorable special treatment to the self-governance of SCDC. Consequently, it must be presumed that SCDC would be subject to the exact same restrictions on agreements covered by Article 101 as all other undertakings in terms of competition law.

Violations of Article 102 – Data as an Essential Facility

As the purpose of a SCDC is to govern the sharing of the data through what is essentially a monopoly, violations of Article 102 TFEU must be considered. Article 102 TFEU is intended to prevent the abuse of a dominant position, especially one that restricts market entry (Persch, 2021, p. 544), therefore, a SCDC gatekeeping the availability of data is *prima facie* in a prime position to be caught by this provision. Furthermore, noted in the EU's strategy for data, the availability and sharing of data is envisioned to not only improve existing services, but additionally develop new goods and services (European Commission, 2020, pp. 2-3). Consequently, in the context of Article 102 TFEU, the 'Essential Facilities Doctrine' (EFD) is arguably relevant, as it pertains to a situation where a monopoly refuses to grant access to a resource that is essential for the development of new products (Tommaso, 2020, p. 196).

Therefore, it is not inconceivable that a SCDC could face legal action following the denial of access to the smart city data. As has been demonstrated above, these decisions may have the capacity to influence the trade between EU MS, whereby it is justified to examine the hypothetical legal conflict from the lens of the EU and the EFD as it is applied in regard to Article 102 TFEU. This does not mean that smart city commons are necessarily free from similar concerns deriving from EU MS law, however, it is impractical to examine all the EU MS national competition law practices in the context of this paper, whereby the focus will be on the EU's interpretation of EFD.

Strictly speaking, in the EU case law, the CJEU refers to "refusals to supply or deal" rather than EFD (Graef, 2019, pp. 41-43), however for the sake of simplicity for this paper the term 'EFD' will be used in their stead. As a test for whether the refusal can be considered abusive, the CJEU uses a cumulative three step test which derives from a number of influential cases such as Magill and Bronner (Ibid, 2019). Under the Bronner criteria, the three steps are that the refusal is (1) not objectively justified, (2) the resource is 'indispensable' and (3) such refusal is likely to eliminate all competition (Czapracka, 2022, p. 278). However, from a data point of view, the caselaw of IMS Health and Microsoft is arguably more relevant, as they pertain directly to the refusal to deal in the context of Intellectual Property Rights (IPR) and data, especially as the ECJ granted access to data (Bruc, 2019, p. 185). Under IMS Health the criteria was characterized in paragraph 38 slightly differently, with firstly that the refusal must be preventing the emergence of a new product for which there is a potential consumer demand. Secondly, that it is

unjustified and thirdly the refusal must be such to exclude any competition on the secondary market.

When applying the IMS Health test to the context of SCDC, it is conceivable that a 'refusal to deal' data could potentially fulfill all three conditions. Although it must be clarified that despite copyright being frequently the focus such as in IMS Health, where the data was protected by copyright specifically, the considerations are considered to apply to all intellectual property (Slepek, 2020, p. 5). Consequently, as databases and data can be subject to both copyright and the EU's sui generis database protection (Bruc, 2019, p. 211), in the context of smart city data, the discussion will utilize the more IPR specific caselaw such as IMS Health and Microsoft.

Due to the the 2007 Microsoft case, it is best to start with the first and third step of the IMS Health test. In the Microsoft case, the General Court (GC) applied a lower threshold, albeit this is yet to be confirmed by the ECJ (Graef, 2019, p. 46). Under the GC's threshold it is sufficient that not all competition on the market is extinguished by a refusal to share a resource, as the 'likely' prevention of 'effective competition' is sufficient. Furthermore, the GC in T-201/04 further considered that it is sufficient that technical development is limited, which is a considerably lower threshold than the prevention of a new product.

Therefore, in the context of SCDC, if the EU's proposition that the sharing of data can develop new products is accepted, then arguably the smart city data for an entire city could plausibly be used to create such new products or services. Alternatively, if the GC's view is confirmed, it is even more likely that the "technical development" may be limited by the refusal to share such data, as for this to be true the data must only be somewhat useful in further developing a product, which based on the EU's strategy's view on the benefits of data would appear to be an almost certainty.

Furthermore, it is difficult to envision an alternative to the vast amount of data that would be collected through the public infrastructure that would constitute a smart city, for arguably the only feasible alternative would be an equivalent privately owned sensor network in the city. However, the latter would amount to not only a manifest waste of resources, similar to the situation with the monopolistic control of railroads that created the EFD in the U.S. (Pitofsky, 2002, p. 446), but it would also be questionable from an ethical point of view as its sole purpose would be to avoid obtaining consent for sharing and using the data. Hence, it is likely that there is not going to be any replacement for access to the data generated by the smart city, even one that is less advantageous. Consequently, it is reasonable to conclude that the first criteria for the EFD test could be fulfilled by a SCDC refusal to share data.

In addition, if the crucial nature of data for the development and emergence of new products is accepted, then it must follow that with a denial of access to said data, it will be difficult to compete. Consequently, it is reasonable to state that the third step of the test, the exclusion of competition on a secondary market, is entirely plausible. While it may be difficult to pinpoint specifically all the goods and services that may be developed or emerge with the use of smart city data, the nature of smart cities jeopardizes competition on any arising market therein without access to the smart city data. Smart city infrastructures provide raw data for markets for services based on data analysis.

Ostrom and Hess proposed in 2007 that the relationship between data, information and knowledge is such that information represents organized data which in turn can be analyzed to create knowledge (Ostrom and Hess, 2007, p. 8). This conversion of firstly organizing the data, and secondly deriving specific useful knowledge, is arguably a valuable economic service, as it can enable businesses that do not have such data analysis capabilities themselves to obtain valuable knowledge that may improve their competitiveness. Consequently, for an undertaking to be able to compete on such a market, arguably they must have access to the raw data itself to begin organizing and analyzing it. Hence, if such an undertaking is denied access, conceivably they cannot compete. As a direct result, should a SCDC bar access to their data to some or even all but one undertaking in this market, it would effectively prevent any competition on this secondary market. Thus, it must be concluded that the second and third condition could be fulfilled by the governance actions of a SCDC, even if the lowered threshold used by the GC in Microsoft is not used.

This therefore leaves only the second step of the test, the objective justification. An accepted objective justification has the possibility of preventing the behavior from being considered a violation of Article 102 (Van der Vijver, 2012, p. 60). There are three possibilities for objective justifications, legitimate business behavior, legitimate public interest objectives and efficiency considerations. At this stage it is worth recalling that while a commons is an undertaking in the meaning of EU competition law, it is not a business, rather it is a collective body for individuals to self-govern a resource, in this case data. While profits may be made, it is not the purpose of a commons, as its activities are not primarily guided by commercial concerns. Consequently, the first and third possible objective justification -legitimate business behavior and efficiency - are not applicable.

The second ground for an objective justification, a legitimate public interest consideration is far more applicable, especially considering the nature of a commons, which is essentially to protect the interests of the individuals that it consists of through the self-governance of the common resource. Furthermore, the ultimate purpose of Article 102 TFEU is to protect the consumers, and as noted earlier, SCDCs essentially consist of consumers. Therefore, as they self-govern access to their local smart city data, it is not unreasonable to argue that their decisions must

be in the public interest.

However, as case law has demonstrated, pleas of public interest are almost uniformly rejected, albeit often based on the facts of the case rather than the idea of public interest itself (Ibid, 2012, p. 66). Therefore, it is difficult to conclude in the abstract how the GC or CJEU would respond to a case involving a SCDC's objective justification of legitimate public interests. Denials could stem from the preferences of the community, rather than more conventionally accepted grounds of public interest such as public safety. This is arguably exacerbated by the notion that is detectable in the EU's strategy for data and the legal framework, that non-personal data is not considered to be capable of negatively influencing individuals, for any data that relates to an individual is protected by the GDPR and hence an individual has control over it.

However, as demonstrated in this paper, non-personal data can hang over a community like a modern sword of Damocles, with its consequences not necessarily being felt immediately, whereby, it may be desirable from a community point of view to not share the data. Such justifications, however, are likely to appear hollow from the perspective of the GC or CJEU, and thus decisions taken by SCDC could fulfill the second step. Consequently, it is entirely possible that refusals to share data by a SCDC could infringe Article 102 of the TFEU as they could fulfill all three criteria in the IMS Health test for an abuse of a dominant position.

Discussion

The vast amount of data that smart cities will produce undoubtedly will change the lives of their inhabitants, who at present are likely to have little say in how that data will be shared. The European legal framework for data does not envision or empower the local community in regard to the data that they will inevitably produce in a smart city, unless it falls under the definition of personal data under the GDPR. On the contrary, under the Open Data Directive, public sector bodies are obliged to make dynamic data gathered by sensors available and open, thereby bypassing the citizens entirely. This presents a unique opportunity to employ the commons theory of Ostrom to remedy the disempowerment of the smart citizens with an alternative that is neither public nor private, in the spirit of her original idea that broke away from the private-public dichotomy.

Nevertheless, in order to employ her theory in a city environment with smart city data, adaptations must be made. For example, the rather informally organized commons simply cannot be used in the context of a smart city, but rather the smart city data commons if they are to be truly empowered, must take on a legal form. In this regard, an interesting future research direction would be the possible legal forms national implementations of (smart city data) commons could take in the various Member States, which could effectively lay down the foundations for actual commons to be established, either experimentally or permanently.

Furthermore, the adoption of legal forms will bring with it considerable legal implications, such as those connected with competition law. The decision to not share data openly has the potential to cause conflict with the EU's competition law, especially articles 101 and 102 TFEU as has been demonstrated in the section above. These conflicts, if unresolved, or solved unfavourably from a commons perspective, have the potential to condemn smart citizens to perpetual disempowerment in regard to non-personal data gathered of them and their local community. Indeed, in light of the case law and the failure of 'green antitrust', the future prospects for a commons are rather grim from the perspective of caselaw, as theoretical violations are not merely plausible, but arguably almost inevitable for any commons that will decide not to share their data freely.

Naturally, there is no way to know what stance the courts will take until there is an attempt to implement a smart city data commons in the future in a smart city. Which is the primary limitation of this paper, as the analysis is based on caselaw that does not pertain to neither commons nor smart cities. Hence, despite the failure of 'green antitrust', there is still the possibility for the EU courts to decide either way. However, it would nevertheless arguably be desirable for the courts to take a favourable view of SCDCs on the basis that their ultimate purpose is the well-being of the smart citizens through self-governance. For by limiting the ability of SCDC to deny sharing of data, the only effect would be to effectively deepen the disempowerment of the local community in regard to the data that they produce and which can have serious negative consequences for both individuals and entire communities.

Conclusion

The EU's strategy for data contains a vision for a single market for data that produces economic benefits on a Union level. Thus, for the vision to work, data must be shared constantly to provide the 'lifeblood' for bringing the vision to life. The smart cities of the future promise to be a treasure trove of data, as the sensors record many parameters of life in the smart city, whereby such smart city data will be crucial for the success of the vision. However, underlying the vision is a presumption that non-personal data, especially from public sources including smart cities, will be shared absent restrictions. As a result, the individual citizen is essentially relegated to the role of a consumer that will receive economic benefits from the sharing of the data, in which despite producing much of the data, has no ultimate say in whether or under what conditions will the data be shared.

Consequently, this "neoliberal" vision for data arguably is in need of counterbalancing, by the empowerment of the

individual citizen in regard to the non-personal data that they produce by inhabiting a smart city. A possible solution is the self-governance of data through commons, whereby the smart citizens that inhabit a city will be empowered to share their data on their own terms.

However, such decisions may infringe the existing EU legal framework, especially if data is not shared either at all or only to certain undertakings. In this regard, there is a looming possibility of a conflict with EU competition law, as such measures may be categorized as abuses of a dominant position. While a commons' purpose is to govern a common resource subject to social dilemmas, in this case data, rather than being a commercial entity, regardless under EU competition law commons will be considered undertakings and be within its scope. Similar to the notion of 'green antitrust', it would appear that commons management of smart city data is unlikely to receive any special treatment in terms of EU competition law despite its objectives. As demonstrated, the commons are unlikely to benefit from any criteria under the current EU competition law framework that would enable them to be excluded from the scope of either Article 101 or 102.

Therefore, it is somewhat ironic that the competition law that is intended to combat the power of 'Big Tech' companies hinders the possible empowerment of consumers through the emergence of smart city data commons which are able to exert meaningful control over their non-personal data. Indeed, considering that the competition is intended to safeguard the welfare of consumers, it is unfortunate that it can also be used to limit possibilities for meaningful control over non-personal data through self-governance initiatives such as smart city data commons. Non-personal data is not necessarily free of consequences to individuals and may hang like a modern sword of Damocles over the inhabitants of a smart city. Hence, as the current EU competition law framework would likely restrict the meaningful governance opportunities of smart city data commons, arguably it is worth reconsidering whether commons really should be within its scope, and it is necessary to protect consumers from their own decisions regarding their data.

References

- Balestrini, M., Rogers, Y., Hassan, C., Creus, J., King, M., Marshall, P. (2017). A City in Common: A Framework to Orchestrate Large-scale Citizen Engagement Around Urban Issues. In: CHL Conference on Human Factors in Computing Systems, [online] Denver, Colorado: ACM Digital Library, 2282-2294. Available at: <https://doi.org/10.1145/3025453.3025915> [Accessed 07.11.2024]
- Beckwith, R., Sherry, J., Prendergast, D. (2019). Data flow in the Smart City: Open Data Versus the Commons. In: De Lange, M., De Waal, M. (eds.). *The Hackable City*. Singapore: Springer Singapore, 205-221.
- Bruc, É. (2019). Data as an essential facility in European law: how to define the "target" market and divert the data pipeline?. *European Competition Journal*, 15(2–3), 177–224. <https://doi.org/10.1080/17441056.2019.1644576>
- Calzada, I. (2018). (Smart) Citizens from Data Providers to Decision-makers? The Case Study of Barcelona. *Sustainability*, 10(9), 1-25. <https://doi.org/10.3390/su10093252>
- CBS News. (2014). Traffic app facing speed bumps in quiet neighbourhoods. [online] CBS News. Available at: <https://www.cbsnews.com/news/waze-traffic-app-causing-controversy-in-quiet-neighborhoods/> [Accessed 07.11.2024].
- Chyi, N., Wu, D. (2023). Community Land Trusts as Knowledge Commons: Challenges and Opportunities. In Frischmann, F., Madison, M., Sanfilippo, M. (eds.). *Governing Smart Cities as Knowledge Commons*. Cambridge: Cambridge University Press, 83-111. <https://doi.org/10.1017/9781108938532.007>
- Czapracka, K. (2022). The Essential Facilities Doctrine and the Bronner Judgement Clarified: Case C-165/19 P Slovak Telekom v Commission. *Journal of European Competition Law & Practice*, 13(4), 278-280. <https://doi.org/10.1093/jeclap/lpab057>
- D'Ignazio, C., Gordon, E., Christoforetti, E. (2019). Sensors and Civics: Towards a Community-centered Smart City. In Cardullo, P., Di Felicianantonio, C., Kitchin, R. (eds.). *The Right to the Smart City*. Bingley: Emerald Publishing Limited, 113-124. <https://doi.org/10.1108/978-1-78769-139-120191008>
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). *Official Journal of the European Union*, L 172. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN> [Accessed 15 March 2023].
- El Khoury, A. (2018). Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data Through Quantum Mechanics. *Erasmus Law Review*, 11(2), 165-177. <https://doi.org/10.5553/ELR.000114>.
- European Commission. (2020). A European strategy for data. 52020DC0066. Brussels: European Commission. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN> [Accessed 15 March 2023].
- Frank, E., Fernández-Montesinos, G. (2020). Smart City = Smart Citizen = Smart Economy?: An Economic Perspective of Smart Cities. In Cornetta, G., Touhafi, A., Muntean, G. (eds.). *Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies*. Pennsylvania: IGI Global, 161-180. <https://doi.org/10.4018/978-1-7998-3817-3.ch007>
- Frischmann, B., Madison, M., Sanfilippo, M. (eds.). (2023). *Governing Smart Cities as Knowledge Commons*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781108837170>.
- Graef, I. (2019). Rethinking the Essential Facilities Doctrine for the EU Digital Economy. *Revue Juridique Themis*, 53(1), 33-72.
- Judgement of 1 July 2008, Motosykletistiki Omospondia Ellados NPID (MOTOE) v Elliniko Dimosio, C-47/07, EU:C:2008:376.
- Judgement of 17 September 2007, Microsoft Corp. v. Commission of the European Communities. T-201/04, EU:T:2007:289.
- Judgement of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, C-582/14 EU:C:2016:779.
- Judgement of 23 April 1991, Klaus Höfner and Fritz Elser v Macrotron GmbH, C-41/90, EU:C:1991:161.

- Judgement of 29 April 2004, IMS Health GmbH & CO. OHG v NDC Health GmbH & Co. KG. C-418/01, EU:C:2004:257.
- Hoffmann, T. (2019). Smart contracts and void declarations of intent. In Proper, H., Stirna, J. (eds.) *Advanced Information Systems Engineering Workshops. CAiSE 2019. Lecture Notes in Business Information Processing*. Cham: Springer, vol 349, 168–175. https://doi.org/10.1007/978-3-030-20948-3_15.
- Kajander, A. (2022). Legal Perspectives on Smart City Data as a Commons. *International and Comparative Law Review*, 22(2), 7-26. <https://doi.org/10.2478/iclr-2022-0012>.
- Knieps, G. (2017). Internet of Things and the Economics of Smart Sustainable Cities. *Competition and Regulation in Network Industries*, 18(1), 115-131. <https://doi.org/10.1177/1783591717736502>.
- Lange, M. (2019). The Right to the Datafied City: Interfacing the Urban Data Commons. In Cardullo, P., Di Feliciano, C., Kitchin, R. (eds). *The Right to the Smart City*. Bingley: Emerald Publishing Limited, 71-83. <https://doi.org/10.1080/1369118X.2021.1909095>.
- Marques, M., Marques, J., Garcia, B., Cortese, T. (2021). Contributions to Knowledge-Based Development Through Commons Theory, Using Data as a Common Good. *Revista de Gestao Ambiental e Sustentabilidade*, 10, 1-25. <https://doi.org/10.5585/geas.v10i2.18231>.
- Morozov, E. Bria, F. (2018). *Rethinking the Smart City Democratizing Urban Technology*, New York: Rosa Luxemburg Stiftung, 1-53.
- Okeoghene, O. (2005). The meaning of Undertaking within 81 EC. *The Cambridge yearbook of European Legal Studies*, 7, 211-241. <https://doi.org/10.1017/S1528887000004996>
- Ostrom, E. (1990). *Governing the Commons*. Cambridge: Cambridge University Press.
- Ostrom, E., Hess, C. (2007). *Understanding Knowledge as a Commons*. Massachusetts: MIT Press.
- Persch, J. (2021). The role of fundamental rights in antitrust law – a special responsibility for undertakings with regulatory power under Art. 102 TFEU? *European Competition Journal*, 17(3), 542-566. <https://doi.org/10.1080/17441056.2021.1970379>.
- Pitofsky, R., et al. (2002). The Essential Facilities Doctrine under U.S. Antitrust Law. *Antitrust Law Journal*, 70(2), 443-462.
- Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, innovation and Technology*, 11(1), 40-81. <https://doi.org/10.1080/17579961.2018.1452176>.
- Raymond, A. Kouper, I. (2023). Open Governments, Open Data Moving toward a Digital Commons Framework. In: Frischmann, F., Madison, M., Sanfilippo, M. (eds.) *Governing Smart Cities as Knowledge Commons* Cambridge: Cambridge University Press, 58-80. <https://doi.org/10.1017/9781108938532.005>
- 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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *OJ L 119* (32016R0679) 4 May. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 15 March 2023].
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. *OJ L 303* (32018R1807), 28 Nov. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807> [Accessed 15 March 2023]
- Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). *OJ L 152* (32022R0868), 3 Jun. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868> [Accessed 15 March 2023].
- Robertson, V. (2018). Consumer Welfare in Financial Services A View from EU Competition Law. *Yearbook of Antitrust and Regulatory Studies*, 11(17), pp. 29-52. <https://doi.org/10.7172/1689-9024.YARS.2018.11.17.2>
- Sauter, W., Schepel, H. (2010). *State and Market in European Union Law*. Cambridge: Cambridge University Press.
- Slepek, V. (2020). Refusal to deal in the field of technologies as a form of abusing of a dominant position in European and Eurasian unions law. *Journal of Physics: Conference Series*, 1685, 1-8.
- Soe, R-M, Ruohomäki, T., Patzig, H. (2022). Urban Open Platform for Borderless Smart Cities. *Applied Sciences*, 12(2), 1-14. <https://doi.org/10.3390/app12020700>
- Tommaso, F. (2020). An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons. *Global Jurist*, 21(1), 181-210. <https://doi.org/10.1515/gj-2020-0034>
- Tropp, E-M., Hoffmann, T., Chochia, A. (2022) Open Data – a stepchild in e-Estonia’s Data Management Strategy? *TalTech Journal of European Studies*, 12 (1), 123–144. <https://doi.org/10.2478/bjes-2022-0006>
- Van der Gronden, J. (2018). Services of General Interest and the Concept of Undertaking: Does EU Competition Law Apply. *World Competition*, 197, 197-223. <https://doi.org/10.54648/woco2018011>
- Van der Vijver, T. (2012). Objective Justification and Article 102 TFEU. *World Competition*, 35(1), 55-76.
- Volkovski, C. (2022). The case against green antitrust. *European Competition Journal*, 18 (3), 401-513. <https://doi.org/10.1080/17441056.2022.2056346>
- Zelger, B. (2022). The new sustainability exemption according to 2(1) Austrian Cartel Act and its relationship with Article 101 TFEU – European spearhead born to fail? *European Competition Journal*, 18 (3), 514-531. <https://doi.org/10.1080/17441056.2022.2131238>
- Zofcinova, V., Cajkova, A., Kral, R. (2022). Local Leader and the Labour Law Position in the Context of the Smart City Concept through the Optics of the EU. *TalTech Journal of European Studies*, 12 (1), 3-25. <https://doi.org/10.2478/bjes-2022-0001>