Technological Forecasting & Social Change

Is there enough trust for the smart city? Exploring acceptance for use of mobile phone data in Oslo and Tallinn

--Manuscript Draft--

Manuscript Number:	TFS_2019_1421R2
Article Type:	Research Paper
Keywords:	trust; smart cities; big data; mobile phone data
Corresponding Author:	Tom Erik Julsrud, Dr Cicero Senter for Klimaforskning Oslo, Norway
First Author:	Tom Erik Julsrud, Dr
Order of Authors:	Tom Erik Julsrud, Dr
	Julie Runde Krogstad, Dr
Abstract:	There are high hopes that a development towards smarter urban environments, backed up by various big data sources, can help solve many of the challenges facing today's large cities .One of the most useful types of data is mobile phone data (MPD), i.e. data that registers and visualizes urban dwellerss' spatial movement based on mobile phones and other portable devices connected to wireless networks. This study explores the acceptance of use of MPD in different areas, and how it is related to different types of trust. Based on a representative survey of citizens in the two smart cities, Oslo and Tallinn, four similar trust cultures are located. The acceptance of use of MPD differed significantly between the trust cultures and, as expected, was significantly stronger in groups with higher levels of trust, either generally or in terms of reliance on technologies. The acceptance of use of MPD for commercial product development was low for all groups. Findings suggest that future users of MPD need to be aware of the significant scepticism toward and rejection of the use of such data in large parts of the population.
Response to Reviewers:	

	Comments	Actions taken
	Reviewer #3	
1	The two case study cities are *very* different in socio-economic respects. I would have expected much more justification for the choice (other than the implicit fact that one is in the home country and the other is 'interesting' because of its national government's digital and economic development policies). In what way might any of the outcomes be generalisable for policy makers elsewhere?;	We have more clearly explained the case selection and comparative method. We chose the cities partly due to pragmatic reasons and partly due to our expectation that the different historical and cultural contexts would more strongly affect the trust cultures among citizens towards the use of MPD. (See section 3.1. p. 4-5) We have more clearly formulated the finding that the socio-economic and cultural differences between Oslo and Tallinn are not very strongly reflected in how citizens view the sharing of positioning data. This indicates that also policy makers elsewhere can make use of the conceptualization of trust cultures established in this paper. (See section 5.1., p. 9)
2	There is very little contextualisation about how trust in the use of mobile phone location data might differ rom any other data that individuals make available through their actions. There is really quite a large literature about this, comparing attitudes to e.g. sharing data with private companies (mobile phone providers, retailer loyalty cars etc) and different arms of the state. Indeed, there is also a reasonably sizeable literature about attitudes to sharing transport data in areas such as car insurance and road pricing; I would have expected to see some of it referred to here for context.	We have now added a new text to include references to adjacent literature where locational data is studied (p.2). We have also included new text referring to results from studies of attitudes to MPD in other areas (p. 10)
3	Third, the text lapses into polemic too often. The references to surveillance capitalism, global IT companies, China etc are rather unsophisticated and in fact undermine the authors' arguments at key points.	These references have now been taken out.

1. Introduction

A growing number of new services, in particular services related to transport and mobility, are dependent on real-time data from citizens. An almost endless variety of new big data sources offer novel opportunities for city planners and politicians to get valuable insights and knowledge about mobility patterns [1, 2]. One of the most useful types of big data is *mobile phone data* (MPD), i.e. data that registers and visualizes urban travellers' spatial movements during the day, based on mobile phones and other portable devices connected to wireless networks.

MPD is currently harvested, analysed and offered to third parties by telecom operators and technology companies (Google, TomTom, Facebook, etc.). In contrast to traditional survey data, this represents "passive data", in the sense that it is not collected through active solicitation, but is generated by phone operators or service providers for other purposes [2]. Several studies have looked at the challenges and risks involved in extensive use of mobility data, in particular issues connected to citizens' privacy [3, 4]. In connection with the General Data Protection Regulation (GDPR), anonymization of MPD is crucial, because the re-identification of individuals must not be possible according to European law. However, full anonymization is challenging, and often decreases the utility of the data, which means that the benefits of the data cannot fully be exploited [5].

Harvesting of big data is a cornerstone in the development of smart cities. Neoliberal urbanism has dominated previous research on smart cities, which can be summarized as a market-based view centred on economic growth [6]. However, recent contributions have focussed on the transition from smart cities to experimental cities and "smart citizens" [6, 7]. This perspective can be seen as a response to the increasing criticism of smart cities as being overly technology-driven and neglecting public and common interests [8, 9]. The introduction of the GDPR in 2018 started a debate on the digital rights of citizens, i.e. about the ownership of data, data privacy and transparency. Furthermore, cities such as Barcelona are in the process of establishing a more democratic data ownership regime, following an experimental city policy framework [6, 10, 11]. The bottom-up perspective on smart cities means developing new ways to include citizens and adopting an inclusive and deliberative framing of citizen participation in the smart city [6]. The voices of citizens are crucial to gaining acceptance and avoiding violations, conflict and distrust, yet few studies take the perspective of the citizens into account [12, 13].

This paper aims to illuminate how citizens perceive the sharing of information about their movements with mobile phone operators and their wider circle of customers, partners and subcontractors. The use of passive data is undoubtedly a challenge to privacy policies, which influence the everyday life of ordinary citizens, and the use of such data cannot be governed top-down and only discussed in expert debates about data protection [14, 15]. The general awareness among the public about the existence and use of such data is also relatively limited [16]. Trust is a key factor in the acceptance of technology-based systems that can be used for surveillance, such as MPD [17-19]. Trust can be based on various sources and processes; it is also volatile and differently distributed between geographical regions, organizations and social groups [20, 21]. In the context of nations and regions the term *trust cultures* has been used to distinguish between societies on the basis of their level of interpersonal trust and shared ethical values [22, 23]. The question is whether there is sufficient trust within modern societies to implement MPD-based tracking. In this paper, we ask the following questions: What types of trust cultures exist in Oslo and Tallinn? To what extent do trust cultures differ between national contexts? How does affiliation with such groups influence acceptance of the use of MPD data? Based on a comparative survey analysis we explore and describe local *trust cultures* that delineate groups holding different views on security, privacy and confidence in third parties and potential users. As we will show, within these cultures there are very different views on the acceptance of MPD. To achieve future acceptance, it will be necessary to seek support from trust cultures that so far have been reluctant to share their positional data.

The following section gives an overview of earlier studies on smart cities, MPD and trust. This is followed by a section describing the methodological approach and data; after which we present the multivariate statistical analysis and findings. Finally, we discuss the evidence and draw conclusions based on the theoretical framework.

2. Smart cities, mobile phone data and trust cultures

2.1. Smart cities

The use of digital data to monitor and track citizens is closely linked to the idea of smart cities. Although it has been researched for over two decades [24] the concept still lacks a concrete definition [8, 25]. The knowledge about smart cities is rapidly growing and extremely fragmented, and lacks intellectual exchange between researchers in the field. In their analysis of the smart city literature, Mora et al. find that the most cited documents

are based on two dominant interpretations of the smart city [24]. The first understands smart cities holistically as combining human, social, cultural, economic, environmental, and technological aspects. The second takes a techno-centric view of them. Reflecting these interpretations, the literature on smart cities has been criticized for being insufficiently nuanced, using one-size-fits-all narratives, and failing to use in-depth empirical studies and comparative research to underpin the arguments [1].

The research on smart cities is still at an early stage of development. Much still focuses on the understanding of smart cities, often providing illustrative case studies of smart city programmes, public documents and debates [9, 13, 26-28]. It is important to recognize that "smart" technologies function on top of already existing structures and actors, at best promoting incremental change [29, 30]. This implies that there is no such thing as a singular "smart city", because cities are heterogeneously structured within different societies. The term smart cities is part of an ongoing debate on where cities are heading. However, as Thomas et al. [12] note, the term is not perceived as inviting inclusive debate, because citizens find it distant and abstract. Investigations in the UK show that few citizens are familiar with the concept of smart cities. A UK survey found that only one in five adults is familiar with the term [16]. Similarly, Thomas et al. found that most of the interviewees were unfamiliar with it. In general, it seems that citizens lack interest in smart cities [12, 29]. However, much of the "smartness" consists of unseen technological infrastructure and objects undetectable by the majority of citizens.

Recent literature on smart cities moves away from the top-down, neo-liberal, market-based, techno-centric view of smart cities and towards an alternative vision reflecting and serving the interests of the citizens. This literature often relates to the research on new governance models that engage citizens beyond traditional forms, such as co-creation [31]. For example, Calzada [7, 10] focuses on data ownership, grass-roots innovations and co-operative service provision models when analysing the digital plan for Barcelona. He asks whether we are going from smart cities to experimental cities, and how citizens become decision makers rather than data providers. Using data ethically in order to protect citizens and involving citizens in decisions on how data is used are issues that cities are currently experimenting with and constantly need to address in the future.

2.2 Mobile phone data

The use of big data is a cornerstone of smart cities. Big data is real-time data that has been generated due to the "digitization of everyday life", as we leave footprints every time we use a device or a digital service [32]. Over time, this generates compilations of structured and unstructured data that can be used for other purposes than initially intended. In the context of urban development, big data differs from traditional data used to understand human mobility, as it consists of real-time data that has been gathered and stored for other purposes. Exploitation of mobile positioning data is currently widely applied in various part of society as digital technology gets more widespread and big-data analytics gets more advanced. Locational data is applied in connection with implementation of smart homes and household grid technology [33], energy services [34], road pricing systems [35], shared mobility coordination systems [36, 37], and car-tracking by insurance companies[38].

There are several kinds of big data, but in transport-related studies one of the most frequently used and discussed types is *mobile phone data* (MPD), which is generated from mobile phone locational systems and the motion systems integrated into smart phones. Location information is generated as a result of a phone's communication with a cellular network maintained and operated by cellular network operators [39]. It can be registered when a user initiates a connection between the phone and the network through one or more cell towers, or by means of regular updates of geographic position based on the user's movement between different towers in a network. In addition, a number of sources for gathering locational data are built into mobile smartphones or other wireless networks in the city. These include GPS receivers in the smartphones, wi-fi positioning, motion systems, and accelerometer functions. Used in combination, these data sources can extract travel behaviour data that is comprehensive and detailed [4]. Such data is increasingly exploited in various mobile phone application used for sports activities, navigation and social networks.

The increased interest in MPD rests on the fact that access to mobile phones has become ubiquitous in every city, town and village in the world. There are now almost five billion mobile phones users, and an estimated 62.9 per cent of the global population already owned a mobile phone in 2016[1]. The mobile phone has become an integral part of everyday life, and it has also become a favourite companion for travellers, used for trip planning, organization and navigating. Studies indicate that mobile devices are widely used while on the move, to get information from websites, read email, watch movies, communicate with friends and much more [40-43]. The new generation of 5G mobile networks and new smart phone models make the tracking of urban populations

[1] https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

even more accurate and accessible [44]. In the current smart cities, data from mobile phones is part of a large web of various big data sources connecting humans and technologies that can increase the value of CDR-data. These include data from smart card readers, information from "blue tooth beacons", traffic data and more.

2.3. Analytical framework: Trust cultures

Acceptance of digital technologies has traditionally been explained as a product of individual motives and attitudes. In innovation studies, social psychological theories are widely applied in studies about adoption of new services in society. In particular, Theory of Planned Behaviour (TBP) [45] and its offshoots such as the Technology Acceptance Model (TAM) and the Unified Technology Acceptance Model (UTAUT) have been influential. Key assumptions in the latter group of theories are that underlying attitudes, expected ease of use, and perceived usefulness of a technology are decisive for acceptance [46, 47]. Though initially developed for the field of information system adoption, these theories have been applied to a number of other fields, including e-government [17], information systems in organizations [48], mobile applications [49] and online shopping [50]. Despite their popularity, the reliability and usefulness of these theories has been questioned, among other things for ignoring the dynamic social aspects of adoption processes [51, 52].

From the perspective of implementation and acceptance of passive data, this type of approach has several weaknesses. While the decision whether to adopt or reject a technology is seen as active and rational in TBP or TAM, this is usually not the case for mobile phone data. Acceptance can be done implicitly by a lack of resistance or simply through the use of services that are based on mobility positioning. In many cases, however, users will not know how their data is used, even when they have downloaded an application and clicked on the accept button. Secondly, the risks of abuse and/or the possible benefits of acceptance are very hard for regular travellers to comprehend when it comes to the use of passive data, due to its high level of complexity. Another issue is that acceptance for sharing of mobile data is not necessarily similar across all domains or situations. Even research using the traditional technology acceptance models has found that they perform differently in different cultural settings, and that some factors may be more or less important in one culture than another [53, 54]. Thus, a single model for acceptance of technologies across cultures tends to obscure the variations and dynamics involved.

From a more sociological point of view, acceptance of a technological system is understood as a product of collective social processes and is closely related to culture [55, 56]. Whether a certain technology is perceived as a threat to privacy or as a benefit to society depends on the particular cultural context and historical narratives that it links up to. Although various definitions exist, cultures can briefly be described as belief systems that shape individuals' schemas about the world around them [57]. Following a cultural sociological approach, interpretation of the meaning, risks and benefits related to smart cities and big data must be seen as part of an ongoing discourse within a culture. The active development of common understanding of phenomena and social events is often described in sociological literature as "framing". "Collective action frames" represent sets of beliefs and meanings that are used to make sense of events and happenings in the world [58-60].

Acceptance of smart city technologies is to a large extent related to possible future benefits of sharing private data with others. This directly evokes the concept of *trust,* which in general terms can be defined as a "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" [61, p. 395]. According to Luhmann [62] trust arises as a demand for "reduction of complexity" and is based on the delegation of decisions and responsibilities. Giving others access to individual mobility data involves trust because it creates a vulnerability that is handled by belief in the positive intentions of others, as a way to handle high complexity. As a social phenomenon, trust operates on different levels. *Generalized trust*, i.e. to what extent people believe that most other people can be trusted, is seen as a particularly important dimension of a national culture, with significant impact on how new innovations, events or social changes are handled [22, 63, 64]. Following Putnam interpersonal trust, together with networks and norms, is a key element in the concept of *social capital* [64]. When people are engaged in establishing social networks and relations, norms and shared values develop. A society is constituted by a well-established network of social relations, and this constitutes a shared resource (i.e. social capital) which is beneficial for the society as a whole [65, p. 65]. Hence, general trust is used by Putnam as an indicator of social capital in societies. Empirical studies have repeatedly documented significant variation in the level of general trust across nations, which is generally explained by cultural differences [66, 67]. *Institutional trust* is slightly different, as it is related to social institutions and is believed to be of particular importance for the stability of societies and cultures [68, 69]. It reflects how secure one feels about a situation because of guarantees, safety nets and other structures, and the belief that things are normal and customary and that everything seems to be in proper order [70]. Relying on advanced technologies and algorithms to handle coordination of urban processes involves an increasing amount of what sometimes is

described as yet another form of trust: systemic trust or *technology based trust* [71]. Although trust in technological systems is of significance in many emerging fields, it can be contested whether this actually accords with the definition of trust given above, or rather falls under the concept of confidence [72].

It is important to recognize that trust is closely linked to risk, because situations involving risk tend to evoke a need for trust. There are many ways to describe risk, but according to recent sociological approaches, risk is a key implication of the emerging modernity with increased reliance on technological systems. Beck [73] describes this as a need to "foresee and control the future consequences of human action, the various unintended consequences of radicalized modernization" (p. 3). The exploitation of digital systems, such as MPD, can be seen as a typical product of a highly developed modern society leading to a new awareness of risk for abuse.

One of the most discussed risks is intrusion into people's privacy, i.e. violation of individuals' or groups' possibility to seclude themselves or keep information about themselves secret. The boundaries and content of what is considered private differ among cultures and individuals, and can also be constrained by situational factors. To some extent, access to information about citizens is a necessary condition for national authorities to be able to protect citizens, coordinate services and enforce legal rights. Throughout history, there has probably always been tension between the individual's right to privacy and the right of the state to protect itself and the community by inquiring into the lives of individual citizens. However, due to the development of digital technology, sensors, network infrastructure and algorithms for analysing big data, the scale of the state's ability to do this has increased rapidly. This has led to warnings about an increased risk of a "panoptic state" [74], that automatically monitors and registers what people are doing, and develops profiles based on multiple different sources.

The framework of *contextual integrity* is a new approach to privacy, where privacy is perceived as a normative concept [75]. When information is transmitted between actors, it occurs within a specific social context containing specific informational norms. The informational norms connected to each transaction will vary across four key parameters: the specific context, the actors involved, the type of information and the principles of transmission. MPD is part of a larger tidal wave of applications and systems that are relevant for the development of smart cities, but also are enveloped in risks of surveillance and intrusion onto privacy rights. As noted by several scholars, the access to and use of MPD raise serious concerns about violation of citizens' privacy [76], although very few studies have investigated this empirically. One exception is a study by Martin and Shilton [77], who looked at privacy expectations for mobile devices. They found that users expect particular data types, such as location, to be used in the contexts of navigation and weather applications, but not to be used for targeted advertising.

Relying on a sociological approach to trust and surveillance, in this paper we will use the term *trust cultures* to describe the collective understandings of trust – in relation to the use of digital data in developing smarter cities – that are found within subgroups in the populations in the cities We draw on previous literature addressing cultures and trust on a national, community and organizational level [20, 63, 64, 66, 78] using the city as a socio-cultural frame. Trust cultures are groups of people with shared opinions, values and attitudes regarding whom and what to trust in a shared social and locational context. Based on the discussion above it is reasonable to believe that trust cultures are different across national cultures, due to their different histories and "frames", but also that there are different cultures within each city. It is also to be expected that the levels of trust within these cultures will differ according to the field where the harvested data is to be used.

[Table 1]

3. Methodological framework and data

3.1 Case study design

This study follows a comparable case research design. Tallinn in Estonia and Oslo in Norway are different socio-economic societies; however, they are relatively small, modern and technologically advanced European capital cities. As the research takes a cultural sociological approach, we expect that the inhabitants in different cultural contexts, i.e. cities, take divergent attitudes in terms of MPD. Although the cities were partly chosen of

pragmatic reasons[2], we expect the comparative design to show how different historical and cultural contexts affect the trust cultures among citizens towards the use of MPD. Cities and regions are complex and it is difficult to select cases exclusively based on similarities or differences[79]. An additional strength of a comparative design is to get crucial insights into the phenomenon or causal configuration of interest[80]. Below, we give some insights on similarities and differences between the case cities as background information for the comparative approach and the findings.

The similarities between the cities as technologically advanced reflects the fact that citizens are experienced and well-informed about the data that they generate. Both countries have high levels of adoption of mobile broadband services, access to Internet in households, and use of Internet on mobile and portable devices (Table 1). Both capitals are taking their first steps towards becoming smart cities that utilize mobility data on a larger scale, and both have populations of well-educated citizens whose mobile phone data has been exploited in recent years. Tallinn and Oslo also both rank high on indicators of smart mobility and smart cities, such as access to digital infrastructure, an integrated transport system and penetration of communication technologies in the population [81].

However, the cities differ in a number of respects that are viewed as important when investigating trust cultures. First, Norway and Oslo have experienced stable economic growth and have a standard of living that is among the highest in the EU region and a well-developed welfare system. Norwegian citizens, according to repeated studies, have high levels of general trust and trust in public institutions, which arguably are crucial factors for further acceptance of many smart city applications [82]. Estonia and Tallinn have lower economic wealth and equity, although the modern Estonian state has experienced rapid economic development after gaining independence from the Soviet Union in 1991. This historical backdrop may have caused suspicion of digital control and surveillance, but also enthusiasm due to the country's shift to a new national leadership and the development of stronger democratic institutions. Cross-national studies have indicated increased levels of trust in the government and public institutions during the last decades, suggesting that this latter line of development has been taking place[83].

Second, the cities have also followed different pathways in their efforts to employ ICT-based services in their urban infrastructure and to improve public government. Estonia has invested heavily in digitalization of civil services and has introduced e-voting and e-citizenry. Norwegian public authorities have taken a somewhat more cautious approach to privacy, and digital information exchange between public authorities is less widespread. The eGovernment platform was reformed in 2007, leading to the establishment of a new agency for public management and eGovernment (Difi). According to the OECD, however, Norway is still struggling to acquire an efficient governance model [84].

Third, harvesting of mobile phone data based on MPD has been tried out in both countries, mainly in the context of research activities supported by telecom operators [44, 85, 86]. Commercialization has been utilized to a larger degree in Estonia. As a consequence, MPD-based data has been made publicly available, and is provided by telecom operators in collaboration with commercial operators[3].

The comparison between the trust cultures of Oslo and Tallinn may reveal the significance of national and cultural context when it comes to the use of MPD data in cities. This is important knowledge for European cities that are struggling with the ethics of data use. Furthermore, findings from these cities, which have different national and cultural contexts, can be relevant for a larger number of similar cities in Europe and the "global north".

3.2 Questionnaire development

The questionnaire was constructed largely using multiple overlapping attitude statements, based on our key research focus and concepts. Agreement with each sub-item was indicated on a five-point scale[4]. A battery of 35 items was designed to capture the key content of the terms trust, risk and acceptance, while at the same time relating this to the harvesting and use of mobile phone data and similar data sources. These items were later reduced to a more limited number of factors based on a factor analysis (PCA).

Acceptance of use of MPD was measured in four areas, to capture how it was related to contexts of use. The following question was asked: "Smart phones can be used to track your mobility pattern. To what extent do you

[2] This contribution is a part of a research project aiming to look at the use of big data in the Norwegian transport sector. Estonian experts were a part of the project, which let us to exploit the opportunity to make a comparative study.

[3] https://www.positium.com/

[4] For the full list of questions, see Appendix.

accept that mobility tracking data could be used in the following areas: research; improvement of transport systems; development of new commercial products or services; protection against terrorism and crime.

Trust was measured in four main areas. To measure general trust, we used a scale to capture both in-group and out-group relationships [87]. In-group trust concerned to what extent the respondents trusted their family, friends and other people whom they knew personally, while out-group trust concerned trust in people with another religion or nationality. These measures represent a more detailed operationalization of the concept of general trust, where a more general form of the question is used to capture general trust in others. For trust on an institutional level, informants were asked to indicate trustfulness toward a list of eleven public and private organizations that in some form or another can be expected to harvest or use MPD through telecom data or mobile applications. This included public health services, banks and insurance companies, telecom operators, domestic revenue services, the police and more. For trust in government, we asked to what extent they trusted the present government, the political parties, the parliament, the justice system, and public authorities. We also asked about whether the government should be given more freedom to harvest and share digital data. To capture the essence of technological and systemic trust, we included questions about confidence in the potential positive benefits of the data system themselves, and their possibilities for producing benefits for the citizens.

Risk was measured by asking respondents whether they thought society has become too vulnerable to terrorist attacks, accidents and catastrophic events, future abuse of personal digital data, and the risk of political surveillance and abuse. We also asked whether they believed stricter regulations were needed to control the use of MPD and similar digital data sources.

3.3 Sample population

The survey questionnaire was distributed to a pre-recruited panel of respondents in each city and was based on a random selection in two strata (adjusted for gender and age). The total net sample included 516 respondents in Oslo and 501 in Tallinn. Table 2 provides an overview of gender and age distributions. The sample was weighted for gender, age and residential area (urban zones) to provide a representative sample for each city. The questionnaire was distributed by email in November 2017[5] (before the introduction of the GDPR). The questionnaires were translated into Estonian, and a Russian version was also available for respondents in Estonia.

[Table 2]

4. Statistical analysis

Before the construction of the cultural sub-groups, a factor analysis was undertaken to identify highly correlated variables and to create a more limited set of variables that could be used in the coming analysis. The factor analysis was conducted separately for each city. In total 35 variables were subjected to a principal component analysis (PCA) with Varimax rotation. A reduced list of components was derived with high level of similarity between the cities – nine in Oslo and six in Tallinn. Factors with eigenvalues below 1 were excluded from further analysis. Each component was reliability tested with a Cronbach's Alpha test to ensure sufficient scale consistency.

The factor component scores were used as input to construct naturally homogeneous groups of people that shared a common conception of trust and possible risks and opportunities related to the use of MPD. For this purpose, a K-means cluster analysis was applied, which is helpful for identifying relatively homogeneous groups of cases based on selected characteristics, using an algorithm that can handle large numbers of cases. Cluster analyses were conducted separately for each city. Since the aim of this analysis was to explore and locate trust cultures, some demographic characteristics were also included: age, gender and educational level. This approach has been used in much segmentation research in the social sciences [88 p. 241]. A four-group cluster solution was selected to capture as much variation as possible, but at the same time to establish groups that were sufficiently homogenous and consistent. Finally, the impact of group membership on acceptance of MPD across five areas was analysed using a regression model.

[5] The informants were selected from Kantar's panel of users, and Kantar also assisted with the sample design and the distribution of the survey.

4.1 Exploring trust cultures

The aim of the factor analysis was to help identify latent structural variables outlining different notions of trust in the use of mobile phone data within each of the cities. We identified nine factors in Oslo and eight in Tallinn, and these were given short labels according to the characteristics of their key content (Table 3). The factors addressed constellations of attitudes, norms and meanings regarding whom to trust in general (institutions, the political systems, individuals) whom to trust with regard to sharing of personal information (web-based enterprises, public institutions, research institutions), particular issues related to risks of abuse, acceptance of countermeasures (stricter rules, more surveillance) and belief in the power of new mobile technologies to improve the city. Two factors were unique to the Norwegian sample (Research & Statistics and Law & Regulations) and one to the Estonian (In-group trust). The latter was excluded due to low scale reliability (alpha > 5).

[Table 3]

Although the common factors had local variations, we view them as representing similar latent structures, and we gave them identical short labels. All factors were used as input to the cluster analysis, where individuals with similar ideas and understandings of trust, risk and privacy were grouped together. The cluster analysis was conducted separately for each city, and four relatively stable groups were derived for each of the samples. Each of the groups contained people with similar conceptions about trust, risk and privacy – what we here describe as trust cultures. Table 4 summarizes the variables' importance for the establishment of the clusters and their significance. A closer look at the groups revealed a significant degree of similarities, and each of the national groups had matching groups in the other city, though with distinct national variations. Thus, the clusters were given the same names, although local variations are evident. These four trust cultures can briefly be described as follows:

Techno trust: This is a group that has strong trust in the possibility to develop better cities and transport systems based on data from digital mobile phone data, while its trust in societal institutions or political bodies is not very high. In both cities this includes about one third of the sample, and members are middle aged or older with good education. There is a difference between the cities, however, related to acceptance of surveillance. In Tallinn they tend to accept surveillance of mobility patterns for the purpose of social goods, but in Norway this group was clearly more sceptical of this, and implicitly valued privacy higher.

General trust: This is a group of people with high trust in societal institutions (health services, police, etc.) and in the political bodies (government, parties). They also share a high general trust in other people in society, such as foreigners and people of another religion, but are reluctant to trust net-based actors. Still, people in this group recognize risks related to the future use of mobility tracking of citizens based on MPD. In general, individuals in this group are well educated. However, the acceptance of surveillance and privacy was different between the cities, with the Tallinn group being more concerned about abuse than the Oslo group. This group included about every third informant in the Norwegian sample, but the corresponding group in the Estonian sample was significantly smaller.

Net-based trust: In both cities there is a group of younger people with lower education who put trust in Internet-based actors, like Google, Facebook and webshops, but have low general trust in political institutions as well in other people. A difference is that those in Oslo had general trust in political institutions and parties.

State distrust: Lastly, in both cities there is a distinct group expressing distrust in the government and political institutions, as well as in other people in general. Citizens in this group see few benefits for society in the implementation and use of technology for improving society. In Norway this group is also characterized by being in favour of stricter rules and regulations for the use of MPD. Even though they have low trust in the state system, they express surprisingly little concern for overt surveillance and abuse. This group consists in general of middle-aged and older citizens (45+). It is almost twice as large in Tallinn as in Oslo.

[Table 4]

Despite distinct local differences, the clusters outline four different groups in the cities that share similar understandings of trust, risk, privacy and use of MPD. In general, they represent cultures where the levels of trust

in others, the political system and technology were differently aligned. The group that trusts net-based operators and the distrusting group represent low-trust cultures, with little interest in possibilities related to exploitation of mobile technologies in the cities. In general, these two groups included more people in Tallinn than Oslo. The general trust group and the techno trust group are both cultures that display a higher level of trust, although with different areas of focus.

4.2. Acceptance of the use of mobility positioning data

Acceptance of mobility tracking was measured by a set of four questions addressing the potential use of mobile phone data for research, improvement of public services, development of commercial services, and protection against crime and terrorism (Table 5). On an average, 43 and 44 per cent respectively of the populations in Oslo and Tallinn agreed, or strongly agreed, with sharing mobility phone data. Thus, a majority of the citizens in both cities were to some degree opposed to it. The area of use with the lowest level of acceptance was development of commercial services and products, with approximately 16% agreeing or strongly agreeing. In contrast, more than 60% in both cities accepted the use of mobility positioning to protect against terrorism and crime, over 50% to develop better public transport, and over 40% for research purposes. On a general level, then, citizens in the two cities were highly aligned on these questions, although the Estonians displayed a slightly higher level of acceptance of the three most important areas. There were no significant differences between the cities across these variables (Chi square > 0.05).

[Table 5]

However, the acceptance of use of MPD differed significantly between the four trust cultures. Overall those in the techno trust and general trust groups were more accepting of its use within the three most accepted areas: transport, research and protection against terrorism and crime (Figures 1 and 2). As expected, acceptance was stronger in groups with higher levels of trust, either generally or in terms of reliance on technologies. The importance ranking showed that use of MPD for commercial product development was of low importance for all groups, but that use for transport improvement was more highly ranked in the Oslo groups. A regression analysis indicates how membership in each of the groups predicted interest in using MPD (converted to a binary independent variable) in the four key areas (Table 6).

[Figure 1, Figure 2, Table 6]

In Oslo, belonging to the trust group significantly explains acceptance of research and transport purposes, while belonging to the general trust group explains use of MPD to protect against terrorism and crime. In Tallinn, belonging to the techno trust and general trust groups was predictive of acceptance of improvement of transport and protection against terrorism and crime.

In sum, this suggests that trust cultures differ significantly in their views on whether they want to share their data with government, urban planners or others. Despite clear national variations, a high degree of similarity was found between the cities, suggesting that the findings may be representative for other cities of the same size and at the same level of development.

5. Discussion and conclusions

The growing awareness of the possibilities afforded by extracting data from mobile phones has contributed to a wave of studies based on analyses of mobility patterns of urban citizens [44, 89]. The possibilities for use seem almost unlimited, as they offer researchers, planners, technology developers and political decision makers instant information about human mobility patterns. Connected to various other sources, knowledge about individuals' present and most likely future behaviour is highly attractive, and is also increasingly accessible due to developments in mobile network technology.

As we have documented in this study, unlimited harvesting of this data is not in agreement with public opinion in general. The majority of citizens in Oslo and Tallinn in general do not accept the use of such applications, even if the purpose is to benefit society. This means that achieving broad acceptance of further implementation and use requires new governance models and ways of involving citizens. To the extent that citizens do accept use of their data, it is to protect their city against terrorism and crime, for the development of transport services and for

research purposes. Use of MPD for the development of commercial products and services is less accepted and approved. European city governments are already becoming aware of their political and institutional power to secure ethical use of data [10]. Dialogue with and engagement of citizens outside the traditional forms of citizen involvement are becoming increasingly important, and as a result knowledge possessed by citizens, not only knowledge about citizens, is being included in political initiatives [90]

Acceptance of sharing positioning data from mobile phones inevitably involves a significant risk of abuse, and needs to be based on some form of trust among the users. As we have documented in Oslo and Tallinn, we find different trust cultures among citizens based on different understandings of whom to trust and the risks involved. While one of the four groups seems to share a high level of general trust in the political system, including institutions that can benefit from such data, two other groups display strong trust related to the technological possibilities. One of the groups, including a large number of young citizens, had high trust in net-based platforms. This may resonate with the argument recently proposed by Rachel Botsman that in the near future, trust will be based on Internet-based peer-to-peer platforms in ways that make social and institutional trust less relevant [91].

The similarities between the two cases indicate that national and cultural contexts are less significant than hypothesized. However, this shows that the findings are robust (i.e. have high external validity) and that similar structures can probably be found in other European cities. In both cities, we see evidence of a younger generation that trusts web-enterprises more than state institutions. The data also suggest that the share of people adhering to a low-trust culture is higher in Tallinn, and that they generally have a lower level of trust in political institutions. This might be possible to trace back to historical political cultures and the lack of durable democratic institutions in the former Eastern Bloc nations. The recent Covid 19 pandemic may serve as an example. Several European countries have developed mobile software applications that track the geographical location of app users in response to the crisis. In Norway, where trust in political institutions is high, almost 30 per cent of the population downloaded the app during 2 months. In June however, the government stopped the app due to privacy concerns from the Norwegian Data Protection Authority. In Estonia, the government has called on nine companies to help with a privacy-preserving approach to develop an app[92].

5.1. Implications for policy

Whether citizens in Oslo and Tallinn will accept further implementation and use of MPD depends on how the issue is framed in public opinion and in the different social cultures and communities. Although Oslo and Tallinn are different societies in many respects, these differences are not very strongly reflected in how the citizens view sharing of data. This indicates that also other cities and policy makers can make use the four trust cultures established in this study, as a basis when finding ways to exploit mobility positioning data in the development of their cities. As we have seen, the typical "trusting citizen" is currently a minority in Oslo and Tallinn. If the citizens consider it safe to share their data and discover the benefits this can have for their mobility and everyday life, they might develop positive attitudes towards sharing their individual data. In light of the Covid 19 pandemic, we experienced that a crisis makes the inhabitants more willing to share their data, even when privacy costs are high. The study shows, however, that in a normal situation there seems to be insufficient general trust among citizens to exploit this on a wider scale.

The findings of this study indicate that city governments should be cautious about exploiting mobile phone data in the development of smart cities. There is significant scepticism among the majority of citizens regarding further use of such data. Unless visions about the smart cities are grounded in the needs and wants of the citizens, such plans are not likely to succeed, and negative understandings and images of a panoptic state may take stronger hold [74]. As warned by Kitchin [1, p 12] without oversight and enforcement concerning possible abuse of data, it is likely that we will see significant resistance and push-back against these types of real-time data gathering.

Building citizen trust regarding the harvesting of MPD will require providing citizens with information about the opportunities afforded by the use of the data as well as the benefits. An important part of doing this is to establish new arenas where people can engage in discussions about the future use of these kinds of data. City governments that want to exploit mobility data should develop new forms for community engagement where all stakeholder groups, including citizens, are represented [93]. For example, city governments can establish urban laboratories involving local communities and volunteer associations, as well as public and private enterprises. Several scholars describe urban experiments as a fruitful way to enable reflexive and multi-dimensional learning in real-life settings [11]. This presupposes that citizens are recognized not as mere passive consumers of services, but as active participants in and potential contributors to the shaping of a "smarter" urban environment [9, 10]. On the other hand, it would also require more fundamental consideration of how to build up trust in different

segments of society, and in particular among those who today largely distrust political institutions. The latter represent a large group of citizens in both Oslo and Tallinn, and many young people are part of cultures that mainly put trust in net-based actors, not in political institutions. Harvesting mobility data demands that policy makers, researchers and technology providers enter into a dialogue with these groups. In the current political climate in Europe, with decreasing levels of trust in political leaders in many countries, this would require significant efforts.[6] One way forward will be to establish arenas and events where boundary-crossing relationships and trust can be developed through face-to-face meetings. As argued by Calzada et al. [15] social capital and trust will suffer as long as smart cities are only based on digital social networks.

5.2. Research contribution

This study contributes to a recent stream of critical social research addressing users' responses to the use of digital technologies for urban development [1, 7, 9, 13, 28, 94-96]. In contrast to the dominant technology-oriented research – typically based on variations of the technology acceptance model – this study focuses on the current cultural understanding within a given social context. This implies that trust is understood as a shared understanding that is developed, sustained or questioned through social interaction within groups and communities, backed up by social institutions.

The advantage of this perspective is that it gives a broader picture of how individuals in a society view issues related to the implementation and use of new digital innovations like MPD. While several recent studies relying on TAM and/or UTAT approaches have found that trust is important for acceptance of new digital technology [19, 49, 97], the different foundations for trust are usually not considered, and neither are the different levels of trust that exist in societies. Thus, the fact that a large part of the citizenry *does not trust* is neglected, as are the variations between cultures, cities and nations.

The findings in this study are evidence that acceptance of the use of MPD is highly sensitive to the particular contexts of its use. Although the majority of citizens are critical, acceptance increases significantly when the purpose has a high perceived social value. At this point, our research supports earlier work indicating that acceptance of the sharing of private data, including positioning data, depends on the context of use [75, 77]. Although we have limited information on such contexts given the design of our survey, we do find indications that citizens' acceptance and concerns regarding privacy differ across situations of use. As argued by Nissenbaum [75], acceptance of the use of privacy data depends on access to information about who the recipients and users of the data are, the information types that are shared, the principles for transmission and the intended uses. Only limited information is currently available to people tracked by mobile positioning systems, and this probably represents a significant barrier to the development of knowledge, norms and meaning in this area. This echoes other studies that have found that attitudes to sharing of locational data to a large degree depends on expected social benefits and the level of trust to the involved organizations [98-100].

Despite the fact that a large part of the population was opposed to sharing of their mobility data, the number of smartphone users using applications that require positioning data was high in our sample[7]. This apparently self-contradictory behaviour can be related to the "privacy paradox" [101, 102]) according to which people continue to use digital data despite knowing about risks related to it. However, many of the current applications for urban travellers, such as real-time routing information and navigation applications are increasingly necessary tools for managing efficiently in cities, making them hard to do without. This may explain why some of the distrusters and net-based trusters in the survey accepted the use of MPD to some degree. It does not follow, however, that they ignore the risk of privacy violations. Studies of young people have found that many intensive users of social media also routinely engage in privacy-protective behaviour [103]. The current study adds to other works that have found that younger people are more aware of the possibilities for abuse of mobile phone data but also more accepting for sharing data [99, 104]

A leading idea in this paper has been that the understanding of risk and trust is based on communication and the development of shared meaning within a group of people. We have presented the concept of trust cultures to conceptualize these groups, and the results indicate that similar cultural groups co-exist in Oslo and Tallinn. In a

[6] According to a recent global survey of trust, over the last two decades we have seen a progressive destruction of trust in societal institutions, a consequence of the 2008 recession, fears about immigration, and economic dislocation caused by globalization and automation [67] Edelman, "Trust Barometer. Executive Summary," no. https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Executive_Summary.pdf, 2019..

[7] This refers to results from the data analysis not presented in the current paper, but see [100] T. E. Julsrud and J. R. Krogstad, "Tracking mobility using mobile phones: What do the citizens think? ," *Inst. of Transp. Ec.,* no. 1658, 2018.

wider context, these four trust cultures can be considered as "ideal types" that can guide further theoretical or empirical work.

As a study of local cultures this study has limitations, because it relies on survey data that can only capture some of the superficial structures of meaning, attitudes and norms in each population. The cultural groups that are outlined in this study should therefore be considered as tentative constructions that need further investigation to be confirmed or redefined. Hopefully, they may trigger interest in further exploration of trust cultures in emerging smart cities in Europe and elsewhere.

Acknowledgments

This research has been supported by the Norwegian Research Council under the Transport 2025 program; grant number 267744.

Literature

[1] R. Kitchin, "The real-time city? Big data and smart urbanism," *GeoJournal* vol. 79, pp. 1-14, 2015.

[2] C. Chen, J. Ma, Y. Suliso, and Y. Liu, "The promises of big data and small data for travel behavior (aka human mobility) analysis," *Transportation Research Part C,* vol. 68, pp. 285-299, 2016.

[3] J. Steenbruggen, E. Tranos, and P. Nijkamp, "Data from mobile phone operators: A tool for smarter cities?," *Telecommunications Policy,* vol. 39, no. 4-5, pp. 335-346, 2014.

[4] Z. Wang, S. Y. He, and Y. Leung, "Applying mobile phone data to travel behaviour research: A literature review," *Travel Behaviour and Society,* vol. 11, pp. 141-155, 2018.

[5] I. Berzina and I. Lauberte, "The model of automation and extension of tourism economic impact assessment in specific regions," *Research for rural development,* vol. 2, pp. 195-202, 2018.

[6] P. Cardullo and R. Kitchin, "Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused' smart cities in Europe," *Environment and Planning C: Politics and Space,* vol. 37, pp. 1-18, 2018.

[7] I. Calzada, "From Smart Cities to Experimental Cities? ," in *Co-Designing Economies in Transition.*, V.Giorgino and Z. Walsh, Eds.: Palgrave Macmillan, Cham, 2018.

[8] R. G. Hollands, ""Will the real smart city please stand up?" " *City* vol. 12, no. 3, pp. 303-320, 2008.

[9] G. Grossi and D. Pianezzi, "Smart cities: Utopia or neoliberal ideology?," *Cities,* vol. 69, pp. 79-85, 2017/09/01/ 2017.

[10] I. Calzada, "(Smart) Citizens from Data Providers to Decision-Makers? The Case Study of Barcelona," *Sustainability,* vol. 10, no. 9, 2018.

[11] J. Evans, A. Karvonen, and R. Raven, "The experimental city. New modes and prospects of urban transformation," in *The Experimental City*, J. Evans, A. Karvonen, and R. Raven, Eds. London: Routledge, 2018.

[12] V. Thomas, D. Wang, L. Mullagh, and N. Dunn, "Where's Wally? In Search of Citizen Perspectives on the Smart City," *Sustainability* vol. 8, no. 2007, 2016.

[13] A. Vanolo, "Is there anybody out there? The place and role of citizens in tomorrow's smart cities," *Futures,* vol. 82, pp. 26-36, 2016/09/01/ 2016.

[14] M. Minkkinen, B. Auffermann, and S. Heinonen, "Framing the future of privacy: citizens´metaphors for privacy in the coming digital society," *European Journal of Futures Research* vol. 5, no. 7, 2017.

[15] I. Calzada and C. Cobo, "Unplugging: Deconstructing the smart city," *Journal of Urban Technology,* vol. 22, no. 1, pp. 23–43, 2015.

[16] IET, "Smart Cities – Time to involve the People. ," vol. Spring 2016, 2016.

[17] F. Bélanger and L. Carter, "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems,* vol. 17, no. 2, pp. 165-176, 2008/06/01/ 2008.
[18] L. Wong, "Trust in E-Commerce: Risk and trust Building," in *Computer-Mediated Relationships and Trust*, L. L. Brennan and V. E. Johnson, Eds. Hershey: IGI Global, 2008, pp. 176-193.
[19] H. Yeh, "The effects of successful ICT-based smart city services: From citizens' perspectives," *Government Information Quarterly,* vol. 34, no. 3, pp. 556-565, 2017/09/01/ 2017.
[20] R. Bachmann and A. Zaheer, "Handbook of Trust Research." Cheltenham, UK: Edward Elgar, 2006, p.^pp. Pages.
[21] I. Markova, P. Linell, and A. Gillespie, "Trust and Distrust in Society," in *Trust & Distrust. Sociocultural Perspectives*, I. Markova and A. Gillespie, Eds. Charlotte, NC: Information Age Publ. , 2008.
[22] F. Fukuyama, *Trust. The Social Virtues and the Creation of Prosperity* (New York, no.). Free Press, 1995, p. .
[23] S. M. Natale, R. P. Hoffman, and G. Hayward, *Business Education and Training: Corporate Structures, Business, and the Management of Values.* (University Press of America). 1998.
[24] L. Mora, R. Bolici, and M. Deakin, "The First Two Decades of Smart-City Research: A Bibliometric Analysis. ," *Journal of Urban Technology,* vol. 24, no. 1, pp. 3-27., 2017.
[25] A. K. Glasmeier and M. Nebiolo, "Thinking about Smart Cities: The Travels of a Policy Idea that Promises a Great Deal, but So Far Has Delivered Modest Results," *Sustainability,* vol. 8, no. 1122; doi:10.3390/su8111122, 2016.
[26] A. Vanolo, "Smart mentality: The Smart City as Disciplinary Strategy," *Urban Studies,* vol. 51, no. 5, pp. 883-898, 2014.
[27] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: definitions, dimensions, performance, and initiatives," *Journal of Urban Technology,* vol. 22, no. 1, pp. 3-21, 2015.
[28] A. Luque-Ayala and S. Marvin, "Developing a critical understanding of smart urbanism?," *Urban Studies,* vol. 1, no. 2, pp. 1-12, 2015.
[29] R. Cowley, S. Joss, and Y. Dayot, "The smart city and its publics: insights from across six UK cities, , DOI:10.1080/17535069.2017.1293150," *Urban Research & Practice,* vol. 11, no. 1, pp. 1-25, 2018.
[30] C. Gaffney and C. Robertson, "Smarter than Smart: Rio de Janeiro's flawed emergence as a smart city. ," *Journal of Urban Technology,,* vol. 25, no. 3, pp. 1466-1853., 2018.
[31] J. Torfing, E. Sørensen, and A. Røiseland, "Transforming the Public Sector Into an Arena for Co-Creation: Barriers, Drivers, Benefits, and Ways Forward," *Administration & Society 51 (5)* vol. 51, no. 5, pp. 795-825, 2016.
[32] J. Dubow, "Big Data and Urban Mobility.," in "ICT," The World Bank, New York2014.
[33] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure," *Cluster Computing* vol. 22, pp. 43–69, 2019.
[34] P. Grünewald and T. Reisch, "The trust gap: Social perceptions of privacy data for energy services in the United Kingdom," *Energy Research & Social Science,* vol. 68, p. 101534, 2020.
[35] M. U. Iqbal and S. Lim, "Designing privacy-aware mobility pricing systems based on user perspective," *Journal of Location Based Services* vol. 1, no. 4, pp. 274-299, 2008.
[36] U. M. Aïvodji, S. Gambs, M.-J. Huguet, and M.-O. Killijian, "Meeting points in ridesharing: A privacy-preserving approach," *72,* pp. 239-253, 2017.
[37] C. D. Cottrill, "MaaS surveillance: Privacy considerations in mobility as a service," *Transportation Research A,* vol. 131, pp. 50-57, 2020.
[38] S. Derikx, G. A. deReuver, and M. Kroesen, "Can privacy concerns for insurance of connected cars be compensated?," *Electronic markets,* vol. 26, no. 1, 2015.
[39] W. Li, R. Long, H. Chen, and J. Geng, "A review of factors influencing consumer intentions to adopt battery electric vehicles," *Renewable and Sustainable Energy Reviews,* vol. 78, pp. 318-328, 2017/10/01/ 2017.

[40] T. E. Julsrud and J. M. Denstadli, "Smartphones, travel time-use, and attitudes to public transport services. Insights from an explorative study of urban dwellers in two Norwegian cities," *International Journal of Sustainable Transportation,* vol. 11, no. 8, pp. 602-610, 2017/09/14 2017.
[41] G. Lyons and K. Chatterjee, "A Human Perspective on the Daily Commute: Costs, Benefits and Trade-offs," *Transportation Reviews,* vol. 28, no. 2, pp. 181-198, 2012.
[42] S. Kenyon and G. Lyons, "Introducing multitasking to the study of travel and ICT: examining its extent and assesing its potential importance," *Transportation Research Part A,* vol. 41, no. 2, pp. 161-175, 2007.
[43] G. Lyons, J. Jain, and D. Holley, "The use of travel time by rail passengers in Great Britain," *Transportation Research Part A,* vol. 41, no. 1, pp. 107-120, 2007.
[44] F. A. Gregersen and E. B. Lunke, *Network data from mobile phones for travel behaviour research* (no. TØI report). Oslo: Institute of Transport Economics, 2018.
[45] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes,* vol. 50, no. 2, pp. 179-211, 1991.
[46] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* vol. 27, pp. 425-478, 2003.
[47] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology " *MIS Quarterly,* vol. 13, no. 3, pp. 319–342., 1989.
[48] M. Horst, M. Kuttschreuter, and J. Gutteling, "Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in the Netherlands," *Computers in Human Behavior,* vol. 23, pp. 1838-1852, 2007.
[49] A. D. Beldad and S. M. Hegner, "Expanding the Technology Acceptance Model with inclusion of Trust, Social Influence, and Health Valuation to Determine the Predictors of German Users Willingness to Continue using a Fitness App: A Structural Equationo Modeling Approach," *International Journal of Human-Computer Interaction,* vol. 34, no. 9, pp. 882-893, 2018.
[50] D. Gefen, E. Karahanna, and D. Straub, "Trust and TAM in Online Shopping: An Integrated Model," *Management Information Systems Quarterly* vol. 27, no. 1, 2003.
[51] P. Legris, J. Ingham, and P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model," *Information & Management,* vol. 40, no. 3, pp. 191-204, 2003/01/01/ 2003.
[52] I. Benbasat and h. Barki, "Quo Vadis, TAM?," *Journal of the Association of Information Systems,* vol. 8, no. 4, pp. 211-218, 2007.
[53] D. Straub, M. Keill, and W. Brenner, "Testing the Technology Acceptance Model Across Cultures: A Three Country Study," *Information and Management,* vol. 31, no. 1, pp. 1-11, 1997.
[54] J. Choi and L. V. Geistfeld, "A cross-cultural investigation of consumer e-shopping adoption," *Journal of Economic Psychology,* vol. 25, no. 6, pp. 821-838, 2004.
[55] M. Wolsink, "Social acceptance revisited: gaps, questionable trends, and an auspicious perspective," *Energy Research & Social Science,* vol. 46, pp. 287-295, 2018.
[56] P. Devine-Wright, S. Batel, O. Aas, B. Sovacool, M. c. Labelle, and A. Ruud, "A conceptual framework for understanding the social acceptance of energy infrastructure: Insights from energy storage," *Energy Policy,* vol. 107, pp. 27-31, 2017.
[57] E. Schein, *Organizational culture and leadership*. San Fransisco: Jossey-Bass, 1985.
[58] P. M. Leonardi, "Innovation Blindness: Culture, Frames, and Cross-Boundary Problem Construction in the Development of New Technology Concepts," *Organizational Science,* vol. 22, no. 2, pp. 347–369, 2011.
[59] R. D. Benford and D. A. Snow, "Framing Processes and Social Movements: An Overview and Assessment," *Annual Review of Sociology,* vol. 26, pp. 611-639, 2000.
[60] E. Goffman, *Frame Analysis: An Essay on the Organization of Experience.k.* New York: Harper Colophon, 1974.
[61] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not So Different After All: A Cross-Disipline View of Trust," *Academy of Management Journal,* vol. 3, no. 23, pp. 393-404, 1998.

[62] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives," in *Trust: Making and Breaking Co-operative Relations*, D. Gambetta, Ed. Oxford: Basil Blackwell, 1988, pp. 94-107.
[63] E. Uslaner, "Trust as a Moral Value," in *Handbook of Social Capital* D. Castiglione, J. W. vanDeth, and G. Wolleb, Eds. Oxford: Oxford University Press, 2006.
[64] R. Putnam, *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon Schuster, 2000.
[65] J. Field, *Social Capital* (Key ideas). London, 2003.
[66] R. Inglehardt and C. Weltzel, *Modernization, Cultural Change, and Democracy. The Human Development Sequence*. London: Cambridge, 2005.
[67] Edelman, "Trust Barometer. Executive Summary," no. https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Executive_Summary.pdf, 2019.
[68] L. G. Zucker, "Production of Trust. Institutional sources of economic structure, 1840-1920," in *Research in Organizational Behavior*, vol. 8, B. M. Staw and L. L. Cummings, Eds. Greenwich: JAI press, 1986, pp. 53-111.
[69] R. Hardin, *Trust*. Cambridge: Polity Press, 2006.
[70] D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Trust formations in new organizational relationships," *Information and Decision Sciences Workshop,* vol. 23, no. 3, pp. 473-490, 1998.
[71] N. Luhmann, *Trust and Power*. New York: Wiley, 1979.
[72] G. Möllering, *Trust: Reason, Routine, Reflexivity*. Amsterdam: Elsevier, 2006.
[73] U. Beck, *World Risk Society*. London: Sage, 1997.
[74] F. Bannister, "The panoptic state: Privacy, surveillance and the balance of risk," *Information Polity,* vol. 10, pp. 65-78, 2005.
[75] H. Nissenbaum, *Privacy in Context – Technology, Policy and the Integrity of Social Life.* . Stanford:: Stanford University Press., 2010.
[76] L. Taylor, "No place to hide? The etics and analytics of tracking mobility using mobile phone data," *Environment and Planning D,* vol. 34, no. 2, pp. 319-336, 2016.
[77] K. Martin and K. Shilton, "Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices," *The Information Society,* vol. 32, no. 3, pp. 200-216, 2016.
[78] C. Heckscher, *Trust in a complex world: enriching community*. Oxford: Oxford University Press, 2015.
[79] J. S. Levy, "Case Studies: Types, Designs, and Logics of Inference " *Conflict Management and Peace Science,* vol. 25, pp. 1-18, 2008.
[80] A. Krehl and S. Weck, "Doing comparative case study research in urban and regional studies: what can be learnt from practice? ," *European Planning Studies,* 2019.
[81] L. R. Caragliu, C. DelBo, and P. Nijkamp, "Smart Cities in Europe," *Journal of Urban Technology,* vol. 18, no. 2, pp. 65-82, 2011.
[82] U. Andreasson, "Tillit - det nordiske guldet," 2017.
[83] S. Zmerli, "Social structure and political trust in Europe. Mapping contextual preconditions of a relational concept," in *Society and Democracy in Europe*: HAL Archives, 2012, pp. 111-138,.
[84] OECD, "Digital Government. Review of Norway," *https://www.oecd.org/gov/digital-government/digital-government-review-norway-recommendations.pdf*, 2018.
[85] R. Ahas, A. Aasa, Ü. Mark, T. Pae, and A. Kull, "Seasonal tourism spaces in Estonia: case study with mobile positioning data," *Tourism Management,* vol. 28, pp. 898-910, 2007.
[86] R. Ahas, A. Aasa, S. Silm, and M. Tiru, "Daily rhythms of suburban commuters´movements in the Tallinn metropolitan area: Case study with mobilepositioning data," *Transportation Research Part C,* vol. 18, pp. 45-54, 2010.
[87] J. Delhey and C. Weltzel, "Generalizing Trust. How Outgroup-Trust Grows Beyond Ingroup-Trust," *World Values Research* vol. 5, no. 3, pp. 46-69., 2012.
[88] E. Mooi and M. Sarstedt, *A Concise Guide to Market Research*. Berlin Heidelberg Springer-Verlag, 2011.

[89] J. Curzon, A. Almehmadi, and K. El-Khatib, "A survey of privacy enhancing technologies for smart cities," *Pervasive and Mobile Computing,* vol. 55, pp. 76-95, 2019.
[90] L. Vesnic-Alujevic, E. Stoermer, J. Rudkin, F. Scapolo, and L. Kimbell, "The Future of Government 2030+. A Citizen Centric Perspective on New Government Models," *Publications Office of the European Union,* no. EUR 29664 2019.
[91] R. Botsman, *Who Can You Trust? How Technology Brought Us Together - and Why It Could Drive Us Apart*. London: Penguin Random House, 2017.
[92] P. H. O'Neil, T. Ryan-Mosley, and B. Johnson, "Covid Tracing Tracker," *MIT Technology Review,* no. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/, 2020.
[93] S. Konsti-Laakso and T. Rantala, "Managing community engagement: A process model for urban planning," *European Journal og operational Research,* vol. InPress, 2017.
[94] A. O. Larsson, "Studying Big Data - ethical and methodological considerations," in *Internet research ethics*, H. Fossheim and H. Ingierd, Eds. oslo: Cappelen Damm, 2015.
[95] D. Boyd, "Critical questions for big data," *Information, communication and society,* vol. 15, no. 5, pp. 662-679, 2012.
[96] C. J. Martin, J. Evans, and A. Karvonen, "Smart and sustainable? Five tensions in the visions and practices of the smart-sustainable city in Europe and North Americ," *Technological Forecasting & Social Change,* vol. 133, pp. 269-278, 2017.
[97] T. Bahmanziari, M. Pearson, and L. Crosby, "Is Trust Important in Technology Adoption? A Policy Capturing Approach," *Journal of Computer Information Systems,* vol. 43, no. 4, pp. 46-54, 2003.
[98] N. Oliver, A. Matic, and E. F. Frias-Martinez, "Mobile network data for public health: Opportunities and challenges," *Frontiers in Public Health,* vol. 38, no. 189, pp. 1-12, 2015.
[99] H. Murphy, L. Keahey, E. Bennett, A. Drake, S. K. Brooks, and G. J. Rubin, "Millennial attitudes towards sharing mobile phone location data with health agencies: a qualitative study," *Information, Communication & Society,* pp. 1468-4462, 2020.
[100] T. E. Julsrud and J. R. Krogstad, "Tracking mobility using mobile phones: What do the citizens think? ," *Inst. of Transp. Ec.,* no. 1658, 2018.
[101] G. Hull, "Successful failure:what Foucault can teach us about privacy self-management in a world of Facebook and big data.," *Ethics Inf Technol,* vol. 17, pp. 89-101, 2015.
[102] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & Security,* vol. 77, pp. 226-261, 2018.
[103] A. E. Marwick and D. Boyd, "Networked Privacy: How Teenagers Negotiate Context in Social Media," *New Media and Society,* vol. 16, no. 7, pp. 1051-1067, 2014.
[104] DMA, *Data privacy: What the consumer really thinks* (no. Direct Marketing Association). London: The direct marketing association, 2018.

Is there enough trust for the smart city? Exploring acceptance for use of mobile phone data in Oslo and Tallinn

Highlights

- Four trust cultures are located in Oslo and Tallinn; Techno trust, General trust, Net-based trust and State distrust
- The acceptance of use of mobile positioning data (MPD) differed significantly between the trust cultures
- The majority of citizens in Oslo and Tallinn in do not accept extensive the use MPD
- The most accepted purposes is to protect against terrorism, development of transport services and for research
- Further implementation and use of MPD requires new governance models and ways of involving citizens

1. Introduction

A growing number of new services, in particular services related to transport and mobility, are dependent on real-time data from citizens. An almost endless variety of new big data sources offer novel opportunities for city planners and politicians to get valuable insights and knowledge about mobility patterns [1, 2]. One of the most useful types of big data is *mobile phone data* (MPD), i.e. data that registers and visualizes urban travellers' spatial movements during the day, based on mobile phones and other portable devices connected to wireless networks.

MPD is currently harvested, analysed and offered to third parties by telecom operators and technology companies (Google, TomTom, Facebook, etc.). In contrast to traditional survey data, this represents "passive data", in the sense that it is not collected through active solicitation, but is generated by phone operators or service providers for other purposes [2]. Several studies have looked at the challenges and risks involved in extensive use of mobility data, in particular issues connected to citizens' privacy [3, 4]. In connection with the General Data Protection Regulation (GDPR), anonymization of MPD is crucial, because the re-identification of individuals must not be possible according to European law. However, full anonymization is challenging, and often decreases the utility of the data, which means that the benefits of the data cannot fully be exploited [5].

Harvesting of big data is a cornerstone in the development of smart cities. Neoliberal urbanism has dominated previous research on smart cities, which can be summarized as a market-based view centred on economic growth [6]. However, recent contributions have focussed on the transition from smart cities to experimental cities and "smart citizens" [6, 7]. This perspective can be seen as a response to the increasing criticism of smart cities as being overly technology-driven and neglecting public and common interests [8, 9]. The introduction of the GDPR in 2018 started a debate on the digital rights of citizens, i.e. about the ownership of data, data privacy and transparency. Furthermore, cities such as Barcelona are in the process of establishing a more democratic data ownership regime, following an experimental city policy framework [6, 10, 11]. The bottom-up perspective on smart cities means developing new ways to include citizens and adopting an inclusive and deliberative framing of citizen participation in the smart city [6]. The voices of citizens are crucial to gaining acceptance and avoiding violations, conflict and distrust, yet few studies take the perspective of the citizens into account [12, 13].

This paper aims to illuminate how *citizens* perceive the sharing of information about their movements with mobile phone operators and their wider circle of customers, partners and subcontractors. The use of passive data is undoubtedly a challenge to privacy policies, which influence the everyday life of ordinary citizens, and the use of such data cannot be governed top-down and only discussed in expert debates about data protection [14, 15]. The general awareness among the public about the existence and use of such data is also relatively limited [16]. Trust is a key factor in the acceptance of technology-based systems that can be used for surveillance, such as MPD [17-19]. Trust can be based on various sources and processes; it is also volatile and differently distributed between geographical regions, organizations and social groups [20, 21]. In the context of nations and regions the term *trust cultures* has been used to distinguish between societies on the basis of their level of interpersonal trust and shared ethical values [22, 23]. The question is whether there is sufficient trust within modern societies to implement MPD-based tracking. In this paper, we ask the following questions: What types of trust cultures exist in Oslo and Tallinn? To what extent do trust cultures differ between national contexts? How does affiliation with such groups influence acceptance of the use of MPD data? Based on a comparative survey analysis we explore and describe local trust cultures that delineate groups holding different views on security, privacy and confidence in third parties and potential users. As we will show, within these cultures there are very different views on the acceptance of MPD. To achieve future acceptance, it will be necessary to seek support from trust cultures that so far have been reluctant to share their positional data.

The following section gives an overview of earlier studies on smart cities, MPD and trust. This is followed by a section describing the methodological approach and data; after which we present the multivariate statistical analysis and findings. Finally, we discuss the evidence and draw conclusions based on the theoretical framework.

2. Smart cities, mobile phone data and trust cultures

2.1. Smart cities

The use of digital data to monitor and track citizens is closely linked to the idea of smart cities. Although it has been researched for over two decades [24] the concept still lacks a concrete definition [8, 25]. The knowledge about smart cities is rapidly growing and extremely fragmented, and lacks intellectual exchange between researchers in the field. In their analysis of the smart city literature, Mora et al. find that the most cited documents

are based on two dominant interpretations of the smart city [24]. The first understands smart cities holistically as combining human, social, cultural, economic, environmental, and technological aspects. The second takes a techno-centric view of them. Reflecting these interpretations, the literature on smart cities has been criticized for being insufficiently nuanced, using one-size-fits-all narratives, and failing to use in-depth empirical studies and comparative research to underpin the arguments [1].

The research on smart cities is still at an early stage of development. Much still focuses on the understanding of smart cities, often providing illustrative case studies of smart city programmes, public documents and debates [9, 13, 26-28]. It is important to recognize that "smart" technologies function on top of already existing structures and actors, at best promoting incremental change [29, 30]. This implies that there is no such thing as a singular "smart city", because cities are heterogeneously structured within different societies. The term smart cities is part of an ongoing debate on where cities are heading. However, as Thomas et al. [12] note, the term is not perceived as inviting inclusive debate, because citizens find it distant and abstract. Investigations in the UK show that few citizens are familiar with the concept of smart cities. A UK survey found that only one in five adults is familiar with the term [16]. Similarly, Thomas et al. found that most of the interviewees were unfamiliar with it. In general, it seems that citizens lack interest in smart cities [12, 29]. However, much of the "smartness" consists of unseen technological infrastructure and objects undetectable by the majority of citizens.

Recent literature on smart cities moves away from the top-down, neo-liberal, market-based, techno-centric view of smart cities and towards an alternative vision reflecting and serving the interests of the citizens. This literature often relates to the research on new governance models that engage citizens beyond traditional forms, such as co-creation [31]. For example, Calzada [7, 10] focuses on data ownership, grass-roots innovations and co-operative service provision models when analysing the digital plan for Barcelona. He asks whether we are going from smart cities to experimental cities, and how citizens become decision makers rather than data providers. Using data ethically in order to protect citizens and involving citizens in decisions on how data is used are issues that cities are currently experimenting with and constantly need to address in the future.

2.2 Mobile phone data

The use of big data is a cornerstone of smart cities. Big data is real-time data that has been generated due to the "digitization of everyday life", as we leave footprints every time we use a device or a digital service [32]. Over time, this generates compilations of structured and unstructured data that can be used for other purposes than initially intended. In the context of urban development, big data differs from traditional data used to understand human mobility, as it consists of real-time data that has been gathered and stored for other purposes. Exploitation of mobile positioning data is currently widely applied in various part of society as digital technology gets more widespread and big-data analytics gets more advanced. Locational data is applied in connection with implementation of smart homes and household grid technology [33], energy services [34], road pricing systems [35], shared mobility coordination systems [36, 37], and car-tracking by insurance companies[38].

There are several kinds of big data, but in transport-related studies one of the most frequently used and discussed types is *mobile phone data* (MPD), which is generated from mobile phone locational systems and the motion systems integrated into smart phones. Location information is generated as a result of a phone's communication with a cellular network maintained and operated by cellular network operators [39]. It can be registered when a user initiates a connection between the phone and the network through one or more cell towers, or by means of regular updates of geographic position based on the user's movement between different towers in a network. In addition, a number of sources for gathering locational data are built into mobile smartphones or other wireless networks in the city. These include GPS receivers in the smartphones, wi-fi positioning, motion systems, and accelerometer functions. Used in combination, these data sources can extract travel behaviour data that is comprehensive and detailed [4]. Such data is increasingly exploited in various mobile phone application used for sports activities, navigation and social networks.

The increased interest in MPD rests on the fact that access to mobile phones has become ubiquitous in every city, town and village in the world. There are now almost five billion mobile phones users, and an estimated 62.9 per cent of the global population already owned a mobile phone in 2016[1]. The mobile phone has become an integral part of everyday life, and it has also become a favourite companion for travellers, used for trip planning, organization and navigating. Studies indicate that mobile devices are widely used while on the move, to get information from websites, read email, watch movies, communicate with friends and much more [40-43]. The new generation of 5G mobile networks and new smart phone models make the tracking of urban populations

[1] https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

even more accurate and accessible [44]. In the current smart cities, data from mobile phones is part of a large web of various big data sources connecting humans and technologies that can increase the value of CDR-data. These include data from smart card readers, information from "blue tooth beacons", traffic data and more.

2.3. Analytical framework: Trust cultures

Acceptance of digital technologies has traditionally been explained as a product of individual motives and attitudes. In innovation studies, social psychological theories are widely applied in studies about adoption of new services in society. In particular, *Theory of Planned Behaviour* (TBP) [45] and its offshoots such as the Technology Acceptance Model (TAM) and the Unified Technology Acceptance Model (UTAUT) have been influential. Key assumptions in the latter group of theories are that underlying attitudes, expected ease of use, and perceived usefulness of a technology are decisive for acceptance [46, 47]. Though initially developed for the field of information system adoption, these theories have been applied to a number of other fields, including e-government [17], information systems in organizations [48], mobile applications [49] and online shopping [50]. Despite their popularity, the reliability and usefulness of these theories has been questioned, among other things for ignoring the dynamic social aspects of adoption processes [51, 52].

From the perspective of implementation and acceptance of passive data, this type of approach has several weaknesses. While the decision whether to adopt or reject a technology is seen as active and rational in TBP or TAM, this is usually not the case for mobile phone data. Acceptance can be done implicitly by a lack of resistance or simply through the use of services that are based on mobility positioning. In many cases, however, users will not know how their data is used, even when they have downloaded an application and clicked on the accept button. Secondly, the risks of abuse and/or the possible benefits of acceptance are very hard for regular travellers to comprehend when it comes to the use of passive data, due to its high level of complexity. Another issue is that acceptance for sharing of mobile data is not necessarily similar across all domains or situations. Even research using the traditional technology acceptance models has found that they perform differently in different cultural settings, and that some factors may be more or less important in one culture than another [53, 54]. Thus, a single model for acceptance of technologies across cultures tends to obscure the variations and dynamics involved.

From a more sociological point of view, acceptance of a technological system is understood as a product of collective social processes and is closely related to *culture* [55, 56]. Whether a certain technology is perceived as a threat to privacy or as a benefit to society depends on the particular cultural context and historical narratives that it links up to. Although various definitions exist, cultures can briefly be described as belief systems that shape individuals' schemas about the world around them [57]. Following a cultural sociological approach, interpretation of the meaning, risks and benefits related to smart cities and big data must be seen as part of an ongoing discourse within a culture. The active development of common understanding of phenomena and social events is often described in sociological literature as "framing". "Collective action frames" represent sets of beliefs and meanings that are used to make sense of events and happenings in the world [58-60].

Acceptance of smart city technologies is to a large extent related to possible future benefits of sharing private data with others. This directly evokes the concept of *trust,* which in general terms can be defined as a "psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" [61, p. 395]. According to Luhmann [62] trust arises as a demand for "reduction of complexity" and is based on the delegation of decisions and responsibilities. Giving others access to individual mobility data involves trust because it creates a vulnerability that is handled by belief in the positive intentions of others, as a way to handle high complexity. As a social phenomenon, trust operates on different levels. *Generalized trust*, i.e. to what extent people believe that most other people can be trusted, is seen as a particularly important dimension of a national culture, with significant impact on how new innovations, events or social changes are handled [22, 63, 64]. Following Putnam interpersonal trust, together with networks and norms, is a key element in the concept of *social capital* [64]. When people are engaged in establishing social networks and relations, norms and shared values develop. A society is constituted by a well-established network of social relations, and this constitutes a shared resource (i.e. social capital) which is beneficial for the society as a whole [65, p. 65]. Hence, general trust is used by Putnam as an indicator of social capital in societies. Empirical studies have repeatedly documented significant variation in the level of general trust across nations, which is generally explained by cultural differences [66, 67]. *Institutional trust* is slightly different, as it is related to social institutions and is believed to be of particular importance for the stability of societies and cultures [68, 69]. It reflects how secure one feels about a situation because of guarantees, safety nets and other structures, and the belief that things are normal and customary and that everything seems to be in proper order [70]. Relying on advanced technologies and algorithms to handle coordination of urban processes involves an increasing amount of what sometimes is

described as yet another form of trust: systemic trust or *technology based trust* [71]. Although trust in technological systems is of significance in many emerging fields, it can be contested whether this actually accords with the definition of trust given above, or rather falls under the concept of confidence [72].

It is important to recognize that trust is closely linked to *risk*, because situations involving risk tend to evoke a need for trust. There are many ways to describe risk, but according to recent sociological approaches, risk is a key implication of the emerging modernity with increased reliance on technological systems. Beck [73] describes this as a need to "foresee and control the future consequences of human action, the various unintended consequences of radicalized modernization" (p. 3). The exploitation of digital systems, such as MPD, can be seen as a typical product of a highly developed modern society leading to a new awareness of risk for abuse.

One of the most discussed risks is intrusion into people's privacy, i.e. violation of individuals' or groups' possibility to seclude themselves or keep information about themselves secret. The boundaries and content of what is considered private differ among cultures and individuals, and can also be constrained by situational factors. To some extent, access to information about citizens is a necessary condition for national authorities to be able to protect citizens, coordinate services and enforce legal rights. Throughout history, there has probably always been tension between the individual's right to privacy and the right of the state to protect itself and the community by inquiring into the lives of individual citizens. However, due to the development of digital technology, sensors, network infrastructure and algorithms for analysing big data, the scale of the state's ability to do this has increased rapidly. This has led to warnings about an increased risk of a "panoptic state" [74], that automatically monitors and registers what people are doing, and develops profiles based on multiple different sources.

The framework of *contextual integrity* is a new approach to privacy, where privacy is perceived as a normative concept [75]. When information is transmitted between actors, it occurs within a specific social context containing specific informational norms. The informational norms connected to each transaction will vary across four key parameters: the specific context, the actors involved, the type of information and the principles of transmission. MPD is part of a larger tidal wave of applications and systems that are relevant for the development of smart cities, but also are enveloped in risks of surveillance and intrusion onto privacy rights. As noted by several scholars, the access to and use of MPD raise serious concerns about violation of citizens' privacy [76], although very few studies have investigated this empirically. One exception is a study by Martin and Shilton [77], who looked at privacy expectations for mobile devices. They found that users expect particular data types, such as location, to be used in the contexts of navigation and weather applications, but not to be used for targeted advertising.

Relying on a sociological approach to trust and surveillance, in this paper we will use the term *trust cultures* to describe the collective understandings of trust – in relation to the use of digital data in developing smarter cities – that are found within subgroups in the populations in the cities We draw on previous literature addressing cultures and trust on a national, community and organizational level [20, 63, 64, 66, 78] using the city as a socio-cultural frame. Trust cultures are groups of people with shared opinions, values and attitudes regarding whom and what to trust in a shared social and locational context. Based on the discussion above it is reasonable to believe that trust cultures are different across national cultures, due to their different histories and "frames", but also that there are different cultures within each city. It is also to be expected that the levels of trust within these cultures will differ according to the field where the harvested data is to be used.

[Table 1]

3. Methodological framework and data

3.1 Case study design

This study follows a comparable case research design. Tallinn in Estonia and Oslo in Norway are different socio-economic societies; however, they are relatively small, modern and technologically advanced European capital cities. As the research takes a cultural sociological approach, we expect that the inhabitants in different cultural contexts, i.e. cities, take divergent attitudes in terms of MPD. Although the cities were partly chosen of

pragmatic reasons[2], we expect the comparative design to show how different historical and cultural contexts affect the trust cultures among citizens towards the use of MPD. Cities and regions are complex and it is difficult to select cases exclusively based on similarities or differences[79]. An additional strength of a comparative design is to get crucial insights into the phenomenon or causal configuration of interest[80]. Below, we give some insights on similarities and differences between the case cities as background information for the comparative approach and the findings.

The similarities between the cities as technologically advanced reflects the fact that citizens are experienced and well-informed about the data that they generate. Both countries have high levels of adoption of mobile broadband services, access to Internet in households, and use of Internet on mobile and portable devices (Table 1). Both capitals are taking their first steps towards becoming smart cities that utilize mobility data on a larger scale, and both have populations of well-educated citizens whose mobile phone data has been exploited in recent years. Tallinn and Oslo also both rank high on indicators of smart mobility and smart cities, such as access to digital infrastructure, an integrated transport system and penetration of communication technologies in the population [81].

However, the cities differ in a number of respects that are viewed as important when investigating trust cultures. First, Norway and Oslo have experienced stable economic growth and have a standard of living that is among the highest in the EU region and a well-developed welfare system. Norwegian citizens, according to repeated studies, have high levels of general trust and trust in public institutions, which arguably are crucial factors for further acceptance of many smart city applications [82]. Estonia and Tallinn have lower economic wealth and equity, although the modern Estonian state has experienced rapid economic development after gaining independence from the Soviet Union in 1991. This historical backdrop may have caused suspicion of digital control and surveillance, but also enthusiasm due to the country's shift to a new national leadership and the development of stronger democratic institutions. Cross-national studies have indicated increased levels of trust in the government and public institutions during the last decades, suggesting that this latter line of development has been taking place[83].

Second, the cities have also followed different pathways in their efforts to employ ICT-based services in their urban infrastructure and to improve public government. Estonia has invested heavily in digitalization of civil services and has introduced e-voting and e-citizenry. Norwegian public authorities have taken a somewhat more cautious approach to privacy, and digital information exchange between public authorities is less widespread. The eGovernment platform was reformed in 2007, leading to the establishment of a new agency for public management and eGovernment (Difi). According to the OECD, however, Norway is still struggling to acquire an efficient governance model [84].

Third, harvesting of mobile phone data based on MPD has been tried out in both countries, mainly in the context of research activities supported by telecom operators [44, 85, 86]. Commercialization has been utilized to a larger degree in Estonia. As a consequence, MPD-based data has been made publicly available, and is provided by telecom operators in collaboration with commercial operators[3].

The comparison between the trust cultures of Oslo and Tallinn may reveal the significance of national and cultural context when it comes to the use of MPD data in cities. This is important knowledge for European cities that are struggling with the ethics of data use. Furthermore, findings from these cities, which have different national and cultural contexts, can be relevant for a larger number of similar cities in Europe and the "global north".

3.2 Questionnaire development

The questionnaire was constructed largely using multiple overlapping attitude statements, based on our key research focus and concepts. Agreement with each sub-item was indicated on a five-point scale[4]. A battery of 35 items was designed to capture the key content of the terms trust, risk and acceptance, while at the same time relating this to the harvesting and use of mobile phone data and similar data sources. These items were later reduced to a more limited number of factors based on a factor analysis (PCA).

Acceptance of use of MPD was measured in four areas, to capture how it was related to contexts of use. The following question was asked: "Smart phones can be used to track your mobility pattern. To what extent do you

[2] This contribution is a part of a research project aiming to look at the use of big data in the Norwegian transport sector. Estonian experts were a part of the project, which let us to exploit the opportunity to make a comparative study.

[3] https://www.positium.com/

[4] For the full list of questions, see Appendix.

accept that mobility tracking data could be used in the following areas: research; improvement of transport systems; development of new commercial products or services; protection against terrorism and crime.

Trust was measured in four main areas. To measure general trust, we used a scale to capture both in-group and out-group relationships [87]. In-group trust concerned to what extent the respondents trusted their family, friends and other people whom they knew personally, while out-group trust concerned trust in people with another religion or nationality. These measures represent a more detailed operationalization of the concept of general trust, where a more general form of the question is used to capture general trust in others. For trust on an institutional level, informants were asked to indicate trustfulness toward a list of eleven public and private organizations that in some form or another can be expected to harvest or use MPD through telecom data or mobile applications. This included public health services, banks and insurance companies, telecom operators, domestic revenue services, the police and more. For trust in government, we asked to what extent they trusted the present government, the political parties, the parliament, the justice system, and public authorities. We also asked about whether the government should be given more freedom to harvest and share digital data. To capture the essence of technological and systemic trust, we included questions about confidence in the potential positive benefits of the data system themselves, and their possibilities for producing benefits for the citizens.

Risk was measured by asking respondents whether they thought society has become too vulnerable to terrorist attacks, accidents and catastrophic events, future abuse of personal digital data, and the risk of political surveillance and abuse. We also asked whether they believed stricter regulations were needed to control the use of MPD and similar digital data sources.

3.3 Sample population

The survey questionnaire was distributed to a pre-recruited panel of respondents in each city and was based on a random selection in two strata (adjusted for gender and age). The total net sample included 516 respondents in Oslo and 501 in Tallinn. Table 2 provides an overview of gender and age distributions. The sample was weighted for gender, age and residential area (urban zones) to provide a representative sample for each city. The questionnaire was distributed by email in November 2017[5] (before the introduction of the GDPR). The questionnaires were translated into Estonian, and a Russian version was also available for respondents in Estonia.

[Table 2]

4. Statistical analysis

Before the construction of the cultural sub-groups, a factor analysis was undertaken to identify highly correlated variables and to create a more limited set of variables that could be used in the coming analysis. The factor analysis was conducted separately for each city. In total 35 variables were subjected to a *principal component analysis* (PCA) with Varimax rotation. A reduced list of components was derived with high level of similarity between the cities – nine in Oslo and six in Tallinn. Factors with eigenvalues below 1 were excluded from further analysis. Each component was reliability tested with a Cronbach's Alpha test to ensure sufficient scale consistency.

The factor component scores were used as input to construct naturally homogeneous groups of people that shared a common conception of trust and possible risks and opportunities related to the use of MPD. For this purpose, a *K-means cluster analysis* was applied, which is helpful for identifying relatively homogeneous groups of cases based on selected characteristics, using an algorithm that can handle large numbers of cases. Cluster analyses were conducted separately for each city. Since the aim of this analysis was to explore and locate trust cultures, some demographic characteristics were also included: age, gender and educational level. This approach has been used in much segmentation research in the social sciences [88 p. 241]. A four-group cluster solution was selected to capture as much variation as possible, but at the same time to establish groups that were sufficiently homogenous and consistent. Finally, the impact of group membership on acceptance of MPD across five areas was analysed using a *regression model.*

[5] The informants were selected from Kantar's panel of users, and Kantar also assisted with the sample design and the distribution of the survey.

4.1 Exploring trust cultures

The aim of the factor analysis was to help identify latent structural variables outlining different notions of trust in the use of mobile phone data within each of the cities. We identified nine factors in Oslo and eight in Tallinn, and these were given short labels according to the characteristics of their key content (Table 3). The factors addressed constellations of attitudes, norms and meanings regarding whom to trust in general (institutions, the political systems, individuals) whom to trust with regard to sharing of personal information (web-based enterprises, public institutions, research institutions), particular issues related to risks of abuse, acceptance of countermeasures (stricter rules, more surveillance) and belief in the power of new mobile technologies to improve the city. Two factors were unique to the Norwegian sample (Research & Statistics and Law & Regulations) and one to the Estonian (In-group trust). The latter was excluded due to low scale reliability (alpha > 5).

[Table 3]

Although the common factors had local variations, we view them as representing similar latent structures, and we gave them identical short labels. All factors were used as input to the cluster analysis, where individuals with similar ideas and understandings of trust, risk and privacy were grouped together. The cluster analysis was conducted separately for each city, and four relatively stable groups were derived for each of the samples. Each of the groups contained people with similar conceptions about trust, risk and privacy – what we here describe as trust cultures. Table 4 summarizes the variables' importance for the establishment of the clusters and their significance. A closer look at the groups revealed a significant degree of similarities, and each of the national groups had matching groups in the other city, though with distinct national variations. Thus, the clusters were given the same names, although local variations are evident. These four trust cultures can briefly be described as follows:

Techno trust: This is a group that has strong trust in the possibility to develop better cities and transport systems based on data from digital mobile phone data, while its trust in societal institutions or political bodies is not very high. In both cities this includes about one third of the sample, and members are middle aged or older with good education. There is a difference between the cities, however, related to acceptance of surveillance. In Tallinn they tend to accept surveillance of mobility patterns for the purpose of social goods, but in Norway this group was clearly more sceptical of this, and implicitly valued privacy higher.

General trust: This is a group of people with high trust in societal institutions (health services, police, etc.) and in the political bodies (government, parties). They also share a high general trust in other people in society, such as foreigners and people of another religion, but are reluctant to trust net-based actors. Still, people in this group recognize risks related to the future use of mobility tracking of citizens based on MPD. In general, individuals in this group are well educated. However, the acceptance of surveillance and privacy was different between the cities, with the Tallinn group being more concerned about abuse than the Oslo group. This group included about every third informant in the Norwegian sample, but the corresponding group in the Estonian sample was significantly smaller.

Net-based trust: In both cities there is a group of younger people with lower education who put trust in Internet-based actors, like Google, Facebook and webshops, but have low general trust in political institutions as well in other people. A difference is that those in Oslo had general trust in political institutions and parties.

State distrust: Lastly, in both cities there is a distinct group expressing distrust in the government and political institutions, as well as in other people in general. Citizens in this group see few benefits for society in the implementation and use of technology for improving society. In Norway this group is also characterized by being in favour of stricter rules and regulations for the use of MPD. Even though they have low trust in the state system, they express surprisingly little concern for overt surveillance and abuse. This group consists in general of middle-aged and older citizens (45+). It is almost twice as large in Tallinn as in Oslo.

[Table 4]

Despite distinct local differences, the clusters outline four different groups in the cities that share similar understandings of trust, risk, privacy and use of MPD. In general, they represent cultures where the levels of trust

in others, the political system and technology were differently aligned. The group that trusts net-based operators and the distrusting group represent low-trust cultures, with little interest in possibilities related to exploitation of mobile technologies in the cities. In general, these two groups included more people in Tallinn than Oslo. The general trust group and the techno trust group are both cultures that display a higher level of trust, although with different areas of focus.

4.2. Acceptance of the use of mobility positioning data

Acceptance of mobility tracking was measured by a set of four questions addressing the potential use of mobile phone data for research, improvement of public services, development of commercial services, and protection against crime and terrorism (Table 5). On an average, 43 and 44 per cent respectively of the populations in Oslo and Tallinn agreed, or strongly agreed, with sharing mobility phone data. Thus, a majority of the citizens in both cities were to some degree opposed to it. The area of use with the lowest level of acceptance was development of commercial services and products, with approximately 16% agreeing or strongly agreeing. In contrast, more than 60% in both cities accepted the use of mobility positioning to protect against terrorism and crime, over 50% to develop better public transport, and over 40% for research purposes. On a general level, then, citizens in the two cities were highly aligned on these questions, although the Estonians displayed a slightly higher level of acceptance of the three most important areas. There were no significant differences between the cities across these variables (Chi square > 0.05).

[Table 5]

However, the acceptance of use of MPD differed significantly between the four trust cultures. Overall those in the techno trust and general trust groups were more accepting of its use within the three most accepted areas: transport, research and protection against terrorism and crime (Figures 1 and 2). As expected, acceptance was stronger in groups with higher levels of trust, either generally or in terms of reliance on technologies. The importance ranking showed that use of MPD for commercial product development was of low importance for all groups, but that use for transport improvement was more highly ranked in the Oslo groups. A regression analysis indicates how membership in each of the groups predicted interest in using MPD (converted to a binary independent variable) in the four key areas (Table 6).

[Figure 1, Figure 2, Table 6]

In Oslo, belonging to the trust group significantly explains acceptance of research and transport purposes, while belonging to the general trust group explains use of MPD to protect against terrorism and crime. In Tallinn, belonging to the techno trust and general trust groups was predictive of acceptance of improvement of transport and protection against terrorism and crime.

In sum, this suggests that trust cultures differ significantly in their views on whether they want to share their data with government, urban planners or others. Despite clear national variations, a high degree of similarity was found between the cities, suggesting that the findings may be representative for other cities of the same size and at the same level of development.

5. Discussion and conclusions

The growing awareness of the possibilities afforded by extracting data from mobile phones has contributed to a wave of studies based on analyses of mobility patterns of urban citizens [44, 89]. The possibilities for use seem almost unlimited, as they offer researchers, planners, technology developers and political decision makers instant information about human mobility patterns. Connected to various other sources, knowledge about individuals' present and most likely future behaviour is highly attractive, and is also increasingly accessible due to developments in mobile network technology.

As we have documented in this study, unlimited harvesting of this data is not in agreement with public opinion in general. The majority of citizens in Oslo and Tallinn in general do not accept the use of such applications, even if the purpose is to benefit society. This means that achieving broad acceptance of further implementation and use requires new governance models and ways of involving citizens. To the extent that citizens do accept use of their data, it is to protect their city against terrorism and crime, for the development of transport services and for

research purposes. Use of MPD for the development of commercial products and services is less accepted and approved. European city governments are already becoming aware of their political and institutional power to secure ethical use of data [10]. Dialogue with and engagement of citizens outside the traditional forms of citizen involvement are becoming increasingly important, and as a result knowledge possessed by citizens, not only knowledge about citizens, is being included in political initiatives [90]

Acceptance of sharing positioning data from mobile phones inevitably involves a significant risk of abuse, and needs to be based on some form of trust among the users. As we have documented in Oslo and Tallinn, we find different trust cultures among citizens based on different understandings of whom to trust and the risks involved. While one of the four groups seems to share a high level of general trust in the political system, including institutions that can benefit from such data, two other groups display strong trust related to the technological possibilities. One of the groups, including a large number of young citizens, had high trust in net-based platforms. This may resonate with the argument recently proposed by Rachel Botsman that in the near future, trust will be based on Internet-based peer-to-peer platforms in ways that make social and institutional trust less relevant [91].

The similarities between the two cases indicate that national and cultural contexts are less significant than hypothesized. However, this shows that the findings are robust (i.e. have high external validity) and that similar structures can probably be found in other European cities. In both cities, we see evidence of a younger generation that trusts web-enterprises more than state institutions. The data also suggest that the share of people adhering to a low-trust culture is higher in Tallinn, and that they generally have a lower level of trust in political institutions. This might be possible to trace back to historical political cultures and the lack of durable democratic institutions in the former Eastern Bloc nations. The recent Covid 19 pandemic may serve as an example. Several European countries have developed mobile software applications that track the geographical location of app users in response to the crisis. In Norway, where trust in political institutions is high, almost 30 per cent of the population downloaded the app during 2 months. In June however, the government stopped the app due to privacy concerns from the Norwegian Data Protection Authority. In Estonia, the government has called on nine companies to help with a privacy-preserving approach to develop an app[92].

5.1. Implications for policy

Whether citizens in Oslo and Tallinn will accept further implementation and use of MPD depends on how the issue is framed in public opinion and in the different social cultures and communities. Although Oslo and Tallinn are different societies in many respects, these differences are not very strongly reflected in how the citizens view sharing of data. This indicates that also other cities and policy makers can make use the four trust cultures established in this study, as a basis when finding ways to exploit mobility positioning data in the development of their cities. As we have seen, the typical "trusting citizen" is currently a minority in Oslo and Tallinn. If the citizens consider it safe to share their data and discover the benefits this can have for their mobility and everyday life, they might develop positive attitudes towards sharing their individual data. In light of the Covid 19 pandemic, we experienced that a crisis makes the inhabitants more willing to share their data, even when privacy costs are high. The study shows, however, that in a normal situation there seems to be insufficient general trust among citizens to exploit this on a wider scale.

The findings of this study indicate that city governments should be cautious about exploiting mobile phone data in the development of smart cities. There is significant scepticism among the majority of citizens regarding further use of such data. Unless visions about the smart cities are grounded in the needs and wants of the citizens, such plans are not likely to succeed, and negative understandings and images of a panoptic state may take stronger hold [74]. As warned by Kitchin [1, p 12] without oversight and enforcement concerning possible abuse of data, it is likely that we will see significant resistance and push-back against these types of real-time data gathering.

Building citizen trust regarding the harvesting of MPD will require providing citizens with information about the opportunities afforded by the use of the data as well as the benefits. An important part of doing this is to establish new arenas where people can engage in discussions about the future use of these kinds of data. City governments that want to exploit mobility data should develop new forms for community engagement where all stakeholder groups, including citizens, are represented [93]. For example, city governments can establish urban laboratories involving local communities and volunteer associations, as well as public and private enterprises. Several scholars describe urban experiments as a fruitful way to enable reflexive and multi-dimensional learning in real-life settings [11]. This presupposes that citizens are recognized not as mere passive consumers of services, but as active participants in and potential contributors to the shaping of a "smarter" urban environment [9, 10]. On the other hand, it would also require more fundamental consideration of how to build up trust in different

segments of society, and in particular among those who today largely distrust political institutions. The latter represent a large group of citizens in both Oslo and Tallinn, and many young people are part of cultures that mainly put trust in net-based actors, not in political institutions. Harvesting mobility data demands that policy makers, researchers and technology providers enter into a dialogue with these groups. In the current political climate in Europe, with decreasing levels of trust in political leaders in many countries, this would require significant efforts.[6] One way forward will be to establish arenas and events where boundary-crossing relationships and trust can be developed through face-to-face meetings. As argued by Calzada et al. [15] social capital and trust will suffer as long as smart cities are only based on digital social networks.

5.2. Research contribution

This study contributes to a recent stream of critical social research addressing users' responses to the use of digital technologies for urban development [1, 7, 9, 13, 28, 94-96]. In contrast to the dominant technology-oriented research – typically based on variations of the technology acceptance model – this study focuses on the current cultural understanding within a given social context. This implies that trust is understood as a shared understanding that is developed, sustained or questioned through social interaction within groups and communities, backed up by social institutions.

The advantage of this perspective is that it gives a broader picture of how individuals in a society view issues related to the implementation and use of new digital innovations like MPD. While several recent studies relying on TAM and/or UTAT approaches have found that trust is important for acceptance of new digital technology [19, 49, 97], the different foundations for trust are usually not considered, and neither are the different levels of trust that exist in societies. Thus, the fact that a large part of the citizenry *does not trust* is neglected, as are the variations between cultures, cities and nations.

The findings in this study are evidence that acceptance of the use of MPD is highly sensitive to the particular contexts of its use. Although the majority of citizens are critical, acceptance increases significantly when the purpose has a high perceived social value. At this point, our research supports earlier work indicating that acceptance of the sharing of private data, including positioning data, depends on the context of use [75, 77]. Although we have limited information on such contexts given the design of our survey, we do find indications that citizens' acceptance and concerns regarding privacy differ across situations of use. As argued by Nissenbaum [75], acceptance of the use of privacy data depends on access to information about who the recipients and users of the data are, the information types that are shared, the principles for transmission and the intended uses. Only limited information is currently available to people tracked by mobile positioning systems, and this probably represents a significant barrier to the development of knowledge, norms and meaning in this area. This echoes other studies that have found that attitudes to sharing of locational data to a large degree depends on expected social benefits and the level of trust to the involved organizations [98-100].

Despite the fact that a large part of the population was opposed to sharing of their mobility data, the number of smartphone users using applications that require positioning data was high in our sample. This apparently self-contradictory behaviour can be related to the "privacy paradox" [101, 102]) according to which people continue to use digital data despite knowing about risks related to it. However, many of the current applications for urban travellers, such as real-time routing information and navigation applications are increasingly necessary tools for managing efficiently in cities, making them hard to do without. This may explain why some of the distrusters and net-based trusters in the survey accepted the use of MPD to some degree. It does not follow, however, that they ignore the risk of privacy violations. Studies of young people have found that many intensive users of social media also routinely engage in privacy-protective behaviour [103]. The current study adds to other works that have found that younger people are more aware of the possibilities for abuse of mobile phone data but also more accepting for sharing data [99, 104]

A leading idea in this paper has been that the understanding of risk and trust is based on communication and the development of shared meaning within a group of people. We have presented the concept of trust cultures to conceptualize these groups, and the results indicate that similar cultural groups co-exist in Oslo and Tallinn. In a wider context, these four trust cultures can be considered as "ideal types" that can guide further theoretical or empirical work.

[6] According to a recent global survey of trust, over the last two decades we have seen a progressive destruction of trust in societal institutions, a consequence of the 2008 recession, fears about immigration, and economic dislocation caused by globalization and automation [67] Edelman, "Trust Barometer. Executive Summary," no. https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Executive_Summary.pdf, 2019..

As a study of local cultures this study has limitations, because it relies on survey data that can only capture some of the superficial structures of meaning, attitudes and norms in each population. The cultural groups that are outlined in this study should therefore be considered as tentative constructions that need further investigation to be confirmed or redefined. Hopefully, they may trigger interest in further exploration of trust cultures in emerging smart cities in Europe and elsewhere.

Acknowledgments

This research has been supported by the Norwegian Research Council under the Transport 2025 program; grant number 267744.

Literature

[1] R. Kitchin, "The real-time city? Big data and smart urbanism," *GeoJournal* vol. 79, pp. 1-14, 2015.
[2] C. Chen, J. Ma, Y. Suliso, and Y. Liu, "The promises of big data and small data for travel behavior (aka human mobility) analysis," *Transportation Research Part C,* vol. 68, pp. 285-299, 2016.
[3] J. Steenbruggen, E. Tranos, and P. Nijkamp, "Data from mobile phone operators: A tool for smarter cities?," *Telecommunications Policy,* vol. 39, no. 4-5, pp. 335-346, 2014.
[4] Z. Wang, S. Y. He, and Y. Leung, "Applying mobile phone data to travel behaviour research: A literature review," *Travel Behaviour and Society,* vol. 11, pp. 141-155, 2018.
[5] I. Berzina and I. Lauberte, "The model of automation and extension of tourism economic impact assessment in specific regions," *Research for rural development,* vol. 2, pp. 195-202, 2018.
[6] P. Cardullo and R. Kitchin, "Smart urbanism and smart citizenship: The neoliberal logic of 'citizen-focused' smart cities in Europe," *Environment and Planning C: Politics and Space,* vol. 37, pp. 1-18, 2018.
[7] I. Calzada, "From Smart Cities to Experimental Cities? ," in *Co-Designing Economies in Transition.*, V.Giorgino and Z. Walsh, Eds.: Palgrave Macmillan, Cham, 2018.
[8] R. G. Hollands, "'Will the real smart city please stand up?' " *City* vol. 12, no. 3, pp. 303-320, 2008.
[9] G. Grossi and D. Pianezzi, "Smart cities: Utopia or neoliberal ideology?," *Cities,* vol. 69, pp. 79-85, 2017/09/01/ 2017.
[10] I. Calzada, "(Smart) Citizens from Data Providers to Decision-Makers? The Case Study of Barcelona," *Sustainability,* vol. 10, no. 9, 2018.
[11] J. Evans, A. Karvonen, and R. Raven, "The experimental city. New modes and prospects of urban transformation," in *The Experimental City*, J. Evans, A. Karvonen, and R. Raven, Eds. London: Routledge, 2018.
[12] V. Thomas, D. Wang, L. Mullagh, and N. Dunn, "Where's Wally? In Search of Citizen Perspectives on the Smart City," *Sustainability* vol. 8, no. 2007, 2016.
[13] A. Vanolo, "Is there anybody out there? The place and role of citizens in tomorrow's smart cities," *Futures,* vol. 82, pp. 26-36, 2016/09/01/ 2016.
[14] M. Minkkinen, B. Auffermann, and S. Heinonen, "Framing the future of privacy: citizens´metaphors for privacy in the coming digital society," *European Journal of Futures Research* vol. 5, no. 7, 2017.
[15] I. Calzada and C. Cobo, "Unplugging: Deconstructing the smart city," *Journal of Urban Technology,* vol. 22, no. 1, pp. 23–43, 2015.
[16] IET, "Smart Cities – Time to involve the People. ," vol. Spring 2016, 2016.
[17] F. Bélanger and L. Carter, "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems,* vol. 17, no. 2, pp. 165-176, 2008/06/01/ 2008.

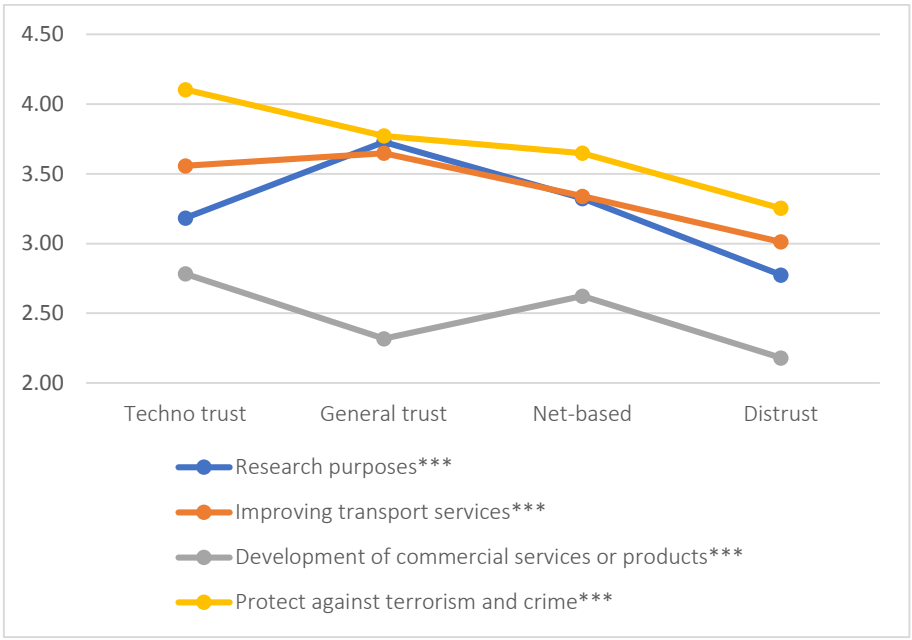
[18] L. Wong, "Trust in E-Commerce: Risk and trust Building," in *Computer-Mediated Relationships and Trust*, L. L. Brennan and V. E. Johnson, Eds. Hershey: IGI Global, 2008, pp. 176-193.
[19] H. Yeh, "The effects of successful ICT-based smart city services: From citizens' perspectives," *Government Information Quarterly,* vol. 34, no. 3, pp. 556-565, 2017/09/01/ 2017.
[20] R. Bachmann and A. Zaheer, "Handbook of Trust Research." Cheltenham, UK: Edward Elgar, 2006, p.^pp. Pages.
[21] I. Markova, P. Linell, and A. Gillespie, "Trust and Distrust in Society," in *Trust & Distrust. Sociocultural Perspectives*, I. Markova and A. Gillespie, Eds. Charlotte, NC: Information Age Publ. , 2008.
[22] F. Fukuyama, *Trust. The Social Virtues and the Creation of Prosperity* (New York, no.). Free Press, 1995, p. .
[23] S. M. Natale, R. P. Hoffman, and G. Hayward, *Business Education and Training: Corporate Structures, Business, and the Management of Values.* (University Press of America). 1998.
[24] L. Mora, R. Bolici, and M. Deakin, "The First Two Decades of Smart-City Research: A Bibliometric Analysis. ," *Journal of Urban Technology,* vol. 24, no. 1, pp. 3-27., 2017.
[25] A. K. Glasmeier and M. Nebiolo, "Thinking about Smart Cities: The Travels of a Policy Idea that Promises a Great Deal, but So Far Has Delivered Modest Results," *Sustainability,* vol. 8, no. 1122; doi:10.3390/su8111122, 2016.
[26] A. Vanolo, "Smart mentality: The Smart City as Disciplinary Strategy," *Urban Studies,* vol. 51, no. 5, pp. 883-898, 2014.
[27] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: definitions, dimensions, performance, and initiatives," *Journal of Urban Technology,* vol. 22, no. 1, pp. 3-21, 2015.
[28] A. Luque-Ayala and S. Marvin, "Developing a critical understanding of smart urbanism?," *Urban Studies,* vol. 1, no. 2, pp. 1-12, 2015.
[29] R. Cowley, S. Joss, and Y. Dayot, "The smart city and its publics: insights from across six UK cities, , DOI:10.1080/17535069.2017.1293150," *Urban Research & Practice,* vol. 11, no. 1, pp. 1-25, 2018.
[30] C. Gaffney and C. Robertson, "Smarter than Smart: Rio de Janeiro's flawed emergence as a smart city. ," *Journal of Urban Technology,,* vol. 25, no. 3, pp. 1466-1853., 2018.
[31] J. Torfing, E. Sørensen, and A. Røiseland, "Transforming the Public Sector Into an Arena for Co-Creation: Barriers, Drivers, Benefits, and Ways Forward," *Administration & Society 51 (5)* vol. 51, no. 5, pp. 795-825, 2016.
[32] J. Dubow, "Big Data and Urban Mobility.," in "ICT," The World Bank, New York2014.
[33] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure," *Cluster Computing* vol. 22, pp. 43–69, 2019.
[34] P. Grünewald and T. Reisch, "The trust gap: Social perceptions of privacy data for energy services in the United Kingdom," *Energy Research & Social Science,* vol. 68, p. 101534, 2020.
[35] M. U. Iqbal and S. Lim, "Designing privacy-aware mobility pricing systems based on user perspective," *Journal of Location Based Services* vol. 1, no. 4, pp. 274-299, 2008.
[36] U. M. Aïvodji, S. Gambs, M.-J. Huguet, and M.-O. Killijian, "Meeting points in ridesharing: A privacy-preserving approach," *72,* pp. 239-253, 2017.
[37] C. D. Cottrill, "MaaS surveillance: Privacy considerations in mobility as a service," *Transportation Research A,* vol. 131, pp. 50-57, 2020.
[38] S. Derikx, G. A. deReuver, and M. Kroesen, "Can privacy concerns for insurance of connected cars be compensated?," *Electronic markets,* vol. 26, no. 1, 2015.
[39] W. Li, R. Long, H. Chen, and J. Geng, "A review of factors influencing consumer intentions to adopt battery electric vehicles," *Renewable and Sustainable Energy Reviews,* vol. 78, pp. 318-328, 2017/10/01/ 2017.

[40] T. E. Julsrud and J. M. Denstadli, "Smartphones, travel time-use, and attitudes to public transport services. Insights from an explorative study of urban dwellers in two Norwegian cities," *International Journal of Sustainable Transportation,* vol. 11, no. 8, pp. 602-610, 2017/09/14 2017.
[41] G. Lyons and K. Chatterjee, "A Human Perspective on the Daily Commute: Costs, Benefits and Trade-offs," *Transportation Reviews,* vol. 28, no. 2, pp. 181-198, 2012.
[42] S. Kenyon and G. Lyons, "Introducing multitasking to the study of travel and ICT: examining its extent and assesing its potential importance," *Transportation Research Part A,* vol. 41, no. 2, pp. 161-175, 2007.
[43] G. Lyons, J. Jain, and D. Holley, "The use of travel time by rail passengers in Great Britain," *Transportation Research Part A,* vol. 41, no. 1, pp. 107-120, 2007.
[44] F. A. Gregersen and E. B. Lunke, *Network data from mobile phones for travel behaviour research* (no. TØI report). Oslo: Institute of Transport Economics, 2018.
[45] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes,* vol. 50, no. 2, pp. 179-211, 1991.
[46] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* vol. 27, pp. 425-478, 2003.
[47] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology " *MIS Quarterly,* vol. 13, no. 3, pp. 319–342., 1989.
[48] M. Horst, M. Kuttschreuter, and J. Gutteling, "Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in the Netherlands," *Computers in Human Behavior,* vol. 23, pp. 1838-1852, 2007.
[49] A. D. Beldad and S. M. Hegner, "Expanding the Technology Acceptance Model with inclusion of Trust, Social Influence, and Health Valuation to Determine the Predictors of German Users Willingness to Continue using a Fitness App: A Structural Equationo Modeling Approach," *International Journal of Human-Computer Interaction,* vol. 34, no. 9, pp. 882-893, 2018.
[50] D. Gefen, E. Karahanna, and D. Straub, "Trust and TAM in Online Shopping: An Integrated Model," *Management Information Systems Quarterly* vol. 27, no. 1, 2003.
[51] P. Legris, J. Ingham, and P. Collerette, "Why do people use information technology? A critical review of the technology acceptance model," *Information & Management,* vol. 40, no. 3, pp. 191-204, 2003/01/01/ 2003.
[52] I. Benbasat and h. Barki, "Quo Vadis, TAM?," *Journal of the Association of Information Systems,* vol. 8, no. 4, pp. 211-218, 2007.
[53] D. Straub, M. Keill, and W. Brenner, "Testing the Technology Acceptance Model Across Cultures: A Three Country Study," *Information and Management,* vol. 31, no. 1, pp. 1-11, 1997.
[54] J. Choi and L. V. Geistfeld, "A cross-cultural investigation of consumer e-shopping adoption," *Journal of Economic Psychology,* vol. 25, no. 6, pp. 821-838, 2004.
[55] M. Wolsink, "Social acceptance revisited: gaps, questionable trends, and an auspicious perspective," *Energy Research & Social Science,* vol. 46, pp. 287-295, 2018.
[56] P. Devine-Wright, S. Batel, O. Aas, B. Sovacool, M. c. Labelle, and A. Ruud, "A conceptual framework for understanding the social acceptance of energy infrastructure: Insights from energy storage," *Energy Policy,* vol. 107, pp. 27-31, 2017.
[57] E. Schein, *Organizational culture and leadership*. San Fransisco: Jossey-Bass, 1985.
[58] P. M. Leonardi, "Innovation Blindness: Culture, Frames, and Cross-Boundary Problem Construction in the Development of New Technology Concepts," *Organizational Science,* vol. 22, no. 2, pp. 347–369, 2011.
[59] R. D. Benford and D. A. Snow, "Framing Processes and Social Movements: An Overview and Assessment," *Annual Review of Sociology,* vol. 26, pp. 611-639, 2000.
[60] E. Goffman, *Frame Analysis: An Essay on the Organization of Experience.k.* New York: Harper Colophon, 1974.
[61] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not So Different After All: A Cross-Disipline View of Trust," *Academy of Management Journal,* vol. 3, no. 23, pp. 393-404, 1998.

[62] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives," in *Trust: Making and Breaking Co-operative Relations*, D. Gambetta, Ed. Oxford: Basil Blackwell, 1988, pp. 94-107.
[63] E. Uslaner, "Trust as a Moral Value," in *Handbook of Social Capital* D. Castiglione, J. W. vanDeth, and G. Wolleb, Eds. Oxford: Oxford University Press, 2006.
[64] R. Putnam, *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon Schuster, 2000.
[65] J. Field, *Social Capital* (Key ideas). London, 2003.
[66] R. Inglehardt and C. Weltzel, *Modernization, Cultural Change, and Democracy. The Human Development Sequence*. London: Cambridge, 2005.
[67] Edelman, "Trust Barometer. Executive Summary," no. https://www.edelman.com/sites/g/files/aatuss191/files/2019-02/2019_Edelman_Trust_Barometer_Executive_Summary.pdf, 2019.
[68] L. G. Zucker, "Production of Trust. Institutional sources of economic structure, 1840-1920," in *Research in Organizational Behavior*, vol. 8, B. M. Staw and L. L. Cummings, Eds. Greenwich: JAI press, 1986, pp. 53-111.
[69] R. Hardin, *Trust*. Cambridge: Polity Press, 2006.
[70] D. H. McKnight, L. L. Cummings, and N. L. Chervany, "Trust formations in new organizational relationships," *Information and Decision Sciences Workshop,* vol. 23, no. 3, pp. 473-490, 1998.
[71] N. Luhmann, *Trust and Power*. New York: Wiley, 1979.
[72] G. Möllering, *Trust: Reason, Routine, Reflexivity*. Amsterdam: Elsevier, 2006.
[73] U. Beck, *World Risk Society*. London: Sage, 1997.
[74] F. Bannister, "The panoptic state: Privacy, surveillance and the balance of risk," *Information Polity,* vol. 10, pp. 65-78, 2005.
[75] H. Nissenbaum, *Privacy in Context – Technology, Policy and the Integrity of Social Life.* . Stanford:: Stanford University Press., 2010.
[76] L. Taylor, "No place to hide? The etics and analytics of tracking mobility using mobile phone data," *Environment and Planning D,* vol. 34, no. 2, pp. 319-336, 2016.
[77] K. Martin and K. Shilton, "Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices," *The Information Society,* vol. 32, no. 3, pp. 200-216, 2016.
[78] C. Heckscher, *Trust in a complex world: enriching community*. Oxford: Oxford University Press, 2015.
[79] J. S. Levy, "Case Studies: Types, Designs, and Logics of Inference " *Conflict Management and Peace Science,* vol. 25, pp. 1-18, 2008.
[80] A. Krehl and S. Weck, "Doing comparative case study research in urban and regional studies: what can be learnt from practice? ," *European Planning Studies,* 2019.
[81] L. R. Caragliu, C. DelBo, and P. Nijkamp, "Smart Cities in Europe," *Journal of Urban Technology,* vol. 18, no. 2, pp. 65-82, 2011.
[82] U. Andreasson, "Tillit - det nordiske guldet," 2017.
[83] S. Zmerli, "Social structure and political trust in Europe. Mapping contextual preconditions of a relational concept," in *Society and Democracy in Europe*: HAL Archives, 2012, pp. 111-138,.
[84] OECD, "Digital Government. Review of Norway," *https://www.oecd.org/gov/digital-government/digital-government-review-norway-recommendations.pdf*, 2018.
[85] R. Ahas, A. Aasa, Ü. Mark, T. Pae, and A. Kull, "Seasonal tourism spaces in Estonia: case study with mobile positioning data," *Tourism Management,* vol. 28, pp. 898-910, 2007.
[86] R. Ahas, A. Aasa, S. Silm, and M. Tiru, "Daily rhythms of suburban commuters´movements in the Tallinn metropolitan area: Case study with mobilepositioning data," *Transportation Research Part C,* vol. 18, pp. 45-54, 2010.
[87] J. Delhey and C. Weltzel, "Generalizing Trust. How Outgroup-Trust Grows Beyond Ingroup-Trust," *World Values Research* vol. 5, no. 3, pp. 46-69., 2012.
[88] E. Mooi and M. Sarstedt, *A Concise Guide to Market Research*. Berlin Heidelberg Springer-Verlag, 2011.

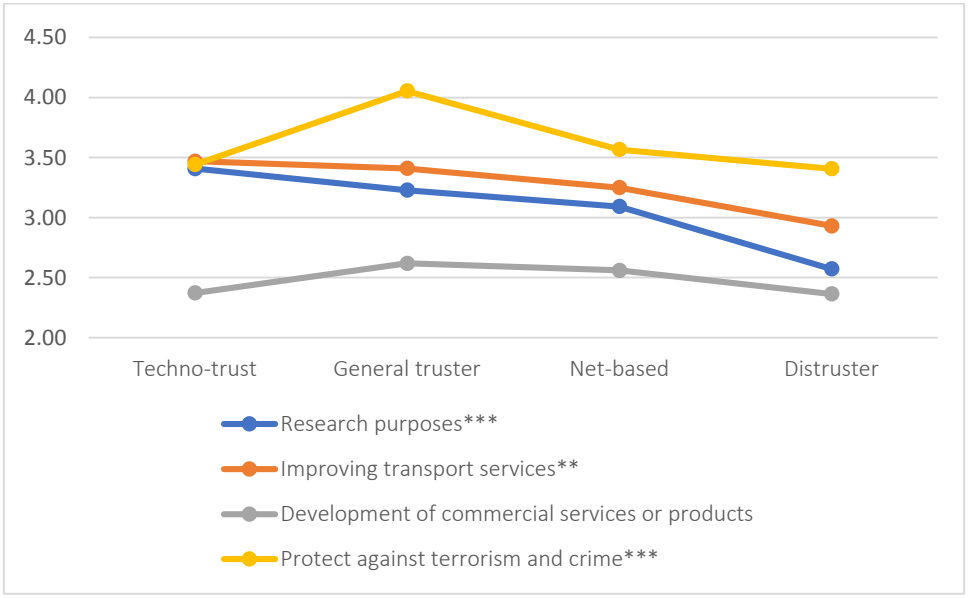
[89] J. Curzon, A. Almehmadi, and K. El-Khatib, "A survey of privacy enhancing technologies for smart cities," *Pervasive and Mobile Computing,* vol. 55, pp. 76-95, 2019.
[90] L. Vesnic-Alujevic, E. Stoermer, J. Rudkin, F. Scapolo, and L. Kimbell, "The Future of Government 2030+. A Citizen Centric Perspective on New Government Models," *Publications Office of the European Union,* no. EUR 29664 2019.
[91] R. Botsman, *Who Can You Trust? How Technology Brought Us Together - and Why It Could Drive Us Apart*. London: Penguin Random House, 2017.
[92] P. H. O'Neil, T. Ryan-Mosley, and B. Johnson, "Covid Tracing Tracker," *MIT Technology Review,* no. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/, 2020.
[93] S. Konsti-Laakso and T. Rantala, "Managing community engagement: A process model for urban planning," *European Journal og operational Research,* vol. InPress, 2017.
[94] A. O. Larsson, "Studying Big Data - ethical and methodological considerations," in *Internet research ethics*, H. Fossheim and H. Ingierd, Eds. oslo: Cappelen Damm, 2015.
[95] D. Boyd, "Critical questions for big data," *Information, communication and society,* vol. 15, no. 5, pp. 662-679, 2012.
[96] C. J. Martin, J. Evans, and A. Karvonen, "Smart and sustainable? Five tensions in the visions and practices of the smart-sustainable city in Europe and North Americ," *Technological Forecasting & Social Change,* vol. 133, pp. 269-278, 2017.
[97] T. Bahmanziari, M. Pearson, and L. Crosby, "Is Trust Important in Technology Adoption? A Policy Capturing Approach," *Journal of Computer Information Systems,* vol. 43, no. 4, pp. 46-54, 2003.
[98] N. Oliver, A. Matic, and E. F. Frias-Martinez, "Mobile network data for public health: Opportunities and challenges," *Frontiers in Public Health,* vol. 38, no. 189, pp. 1-12, 2015.
[99] H. Murphy, L. Keahey, E. Bennett, A. Drake, S. K. Brooks, and G. J. Rubin, "Millennial attitudes towards sharing mobile phone location data with health agencies: a qualitative study," *Information, Communication & Society,* pp. 1468-4462, 2020.
[100] T. E. Julsrud and J. R. Krogstad, "Tracking mobility using mobile phones: What do the citizens think? ," *Inst. of Transp. Ec.,* no. 1658, 2018.
[101] G. Hull, "Successful failure:what Foucault can teach us about privacy self-management in a world of Facebook and big data.," *Ethics Inf Technol,* vol. 17, pp. 89-101, 2015.
[102] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & Security,* vol. 77, pp. 226-261, 2018.
[103] A. E. Marwick and D. Boyd, "Networked Privacy: How Teenagers Negotiate Context in Social Media," *New Media and Society,* vol. 16, no. 7, pp. 1051-1067, 2014.
[104] DMA, *Data privacy: What the consumer really thinks* (no. Direct Marketing Association). London: The direct marketing association, 2018.

Figure



*** ANOVA Sig .< 0.001

Fig. 1. Acceptance of MPD and trust culture, Tallinn. Mean values (1 to 5)



*** ANOVA Sig .< 0.001

Fig. 2. Acceptance of MPD and trust culture, Oslo. Mean values (1 to 5)

Table

Author biography

Dr. *Tom Erik Julsrud* is sociologist and works as a Senior Research Scientist at CICERO Center for International Climate Research. His current research interests include social practice theory, sustainable consumption, socio-technical innovation theory, trust and collaborative consumption. He has recently published the book; *Trust in network organizations*, at Fagbokforlaget (2018).

Julie Runde Krogstad (MA) is a Political Scientist Senior Researcher at TØI – Institute of Transport Economics in Oslo. Her research interests include smart mobility, governance of mobility, and public sector reforms in the transport sector.

Author statement

Paper:	Is there enough trust for the smart city? Exploring acceptance for use of mobile phone data in Oslo and Tallinn
Journal:	Technological Forecasting and Social Change

Contribution from authors:

Tom Erik Julsrud:	Conceptualization, methodology development, data analysis, writing of text
Julie Runde Krogstad:	Literature review, writing of text, editing