The Metaverse as a Virtual Form of Data-Driven Smart Urbanism: On Post-Pandemic Governance through the Prism of the Logic of Surveillance Capitalism

Simon Elias Bibri [1,2,*] **and Zaheer Allam** [3,4]

1   Department of Computer Science, Norwegian University of Science and Technology, Sem Saelands Veie 9, NO-7491 Trondheim, Norway
2   Department of Architecture and Planning, Norwegian University of Science and Technology, Alfred Getz Vei 3, Sentralbygg 1, 5th Floor, NO-7491 Trondheim, Norway
3   Chaire Entrepreneuriat Territoire Innovation (ETI), IAE Paris—Sorbonne Business School, Université Paris Panthéon-Sorbonne, 75013 Paris, France; zaheerallam@gmail.com
4   Live+Smart Research Lab, School of Architecture and Built Environment, Deakin University, Geelong, VIC 3220, Australia
*   Correspondence: simoe@ntnu.no

Abstract: The Metaverse, as a gigantic ecosystem application enabled mainly by Artificial Intelligence (AI), the IoT, Big Data, and Extended Reality (XR) technologies, represents an idea of a hypothetical "parallel virtual environment" that incarnates ways of living in virtually inhabitable cities. It is increasingly seen as a transition from smart cities to virtual cities and a new target for city governments to attain "new" goals. However, the Metaverse project was launched amid the COVID-19 pandemic, a crisis purported to be a rare opportunity that should be seized to reset and reimagine the world—though mainly in regard to its digital incarnation, and what this entails in terms of both cementing and normalizing the corporate-led, top-down, technocratic, tech-mediated, algorithmic mode of governance, as well as new forms of controlling ways of living in urban society. The "new normal" has already set the stage for undemocratically resetting and unilaterally reimagining the world, resulting in an abrupt large-scale digital transformation of urban society, a process of digitization and digitalization that is in turn paving the way for a new era of merging virtuality and urbanity. This has raised serious concerns over the risks and impacts of the surveillance technologies that have been rapidly and massively deployed in the wake of the COVID-19 pandemic. These concerns also relate to the global architecture of the computer mediation of the Metaverse upon which the logic of surveillance capitalism depends, and which is constituted by control and commodification mechanisms that seek to monitor, predict, control, and trade the behavior of human users, as well as to exile them from their own. This viewpoint paper explores and questions the Metaverse from the prism of the social and economic logic of surveillance capitalism, focusing on how and why the practices of the post-pandemic governance of urban society are bound to be undemocratic and unethical. The novelty of the viewpoint lies in providing new insights into understanding the dark side of the ostensible fancier successor of the Internet of today, thereby its value and contribution to the ongoing scholarly debates in the field of Science, Technology, and Society (STS). In addition, by shedding light on the emergence of the Metaverse as a computing platform, the viewpoint seeks to help policymakers understand and assess the ramifications of its wide adoption, as well as to help users make informed decisions about its usage in everyday activity—if it actualizes.

Keywords: Metaverse; data-driven smart urbanism; governance; COVID-19 pandemic; surveillance capitalism; democracy; privacy; civil liberties; datafication; algorithmization; platformization

1. Introduction

The Metaverse has been made possible by the rapid pace of progress in the development of the core enabling technologies, notably Artificial Intelligence (AI), big data, the

Internet of Things (IoT), edge computing, blockchain, Digital Twins (DT), Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), and high-speed 5G networks. While these technologies are not of equal importance in terms of enabling the Metaverse as a "sophisticated" computing platform, their convergence has expedited the connection and integration of the independent virtual spaces owned by various high-tech and platform companies into one cyberspace. In this respect, Meta (formerly Facebook) describes the Metaverse as "a set of virtual spaces where you can create and explore with other people who are not in the same physical space as you. You will be able to hang out with friends, work, play, learn, shop, create, and more" [1]. In short, this vision incarnates ways of living in virtually inhabitable cities of the future. Studying the effects that the emergence of virtual cities has on their perceptions compared to real-world cities, Hemmati [2] found that the Metaverse can create more believable images than reality. However, the Metaverse is not a universal digital experience yet, although it has the potential to interlock, subsume, and afford presence with others, and to easily funnel users from one digital space to another. For a comprehensive state-of-the-art review of the Metaverse with respect to its technological pillars and ecosystem applications and the proposal of a research agenda for its development, the interested reader might be directed to Lee et al. [3].

The research and development of the Metaverse has recently become a key trend in data-driven smart urbanism in terms of the design of virtual cities or digital twin cities using large-scale data-driven AI systems. Much of the rhetoric around the Metaverse echoes the utopian urban visions that emerged in the 1990s. Speculative fiction plays an important role in shaping alternatives to the imaginaries of smart cities [4]. Most of the technologies underlying the Metaverse ecosystem application are associated with the "horizontal information platform" for data-driven smart cities (e.g., [5–7]), which serves to link together diverse smart technologies and solutions to coordinate urban systems and connect things and people. In order for the Metaverse to function properly with respect to virtual services and operational governance in the digital environment, it should coordinate and exchange information with the various spheres of the city administration. As a technological vision, the Metaverse depicts the peculiar characteristics of the experience of everyday life in data-driven smart cities of the future [8]. Urbanism denotes "the distinctive features of the experience of everyday life in cities" ([9], p. 106) which are highly responsive to a form of data-driven urbanism—and whose digitalization, algorithmization, and platformization are being noticeably accelerated and intensified due to the COVID-19 pandemic. The radical expansion of the granularity, range, and magnitude of urban big data and data-intensive compute algorithms combined with the onset of new AI techniques have become compounded by the COVID-19 pandemic. This crisis has proven to be impactful on many levels, thereby inducing big tech companies to look for new ways to cater for the growing demand in the speed, scale, and extension of AI-software computer applications and systems that demand a large amount of computation towards large-scale data-driven AI systems, given their potential for enabling "sophisticated" forms of governance [8,10].

As a virtual form of data-driven smart urbanism—in the sense of "ways of living in cities" [11] or "social relationships in cities" [12]—the Metaverse claims a supremacy of advanced technologies and solutions for achieving numerous benefits across various domains of urban life. By the strategic use of digital infrastructure and big data technologies, smart urbanism seeks to create smart forms of living, mobility, environments, people, economy, and government [13], which are claimed to be integral to the Metaverse as well [14]. However, as argued by Viitanen and Kingston [15], the strategies and solutions of smart cities are based on "technological orthodoxies which are conceptually and empirically shallow". Accordingly, there is a lack of a theoretical basis and empirical evidence required to holistically assess the potential risks and hidden pitfalls of the transformative processes of smart urbanism with respect to the practices, operations, and institutions of urban society [16]. In particular, cities are cast as being "bounded, knowable, and manageable systems that can be steered and controlled in mechanical, linear ways" ([6], p.11). This implies that there is a lack of consideration of the experience of everyday life in the current

model of smart urbanism because it confines urban ways of living to the administrative boundaries of city systems (Verrest and Pfeffer 2019 [17]). In smart urbanism, "both cities and citizens become functional datasets to be managed and manipulated" in order to control urban governance and urban ways of living (Marvin, Luque-Ayala and McFarlane 2015, p. 425) [18]. Numerous studies have, from a variety of perspectives, addressed the negative implications and potential risks of smart urbanism and the ramifications of the pervasion of socially disruptive technologies into the fabric of everyday life—with regard to technocratic governance, governance corporatization, surveillance, privacy, control, and so forth (see Bibri 2021a,b for a comprehensive overview) [16,19]. These are also associated with the global architecture of the computer mediation of the Metaverse upon which the logic of surveillance capitalism depends. Therefore, there is a growing criticism, mistrust, and skepticism of the idea of the Metaverse and its core enabling and driving technologies (e.g., [3,8,20–23]).

2. The Escalating Trends Driving Smart Cities and the Global Architecture of the Computer Mediation of the Metaverse

We are moving into an era where hyper-connectivity, datafication, algorithmization, and platformization pervade the very fabric of urban society as a whole. As a consequence, urban services and urban operational governance are highly responsive to a form of data-driven urbanism; systems, devices, things, and processes are much more tightly interlinked; and citizens are intensively monitored and constantly surveilled. The latter results in generating vast troves of personal data that are analyzed, repackaged, and manipulated to manage, control, and regulate urban ways of living. This is opening up huge opportunities for big tech companies to profiteer from harvesting and exploiting these data. The escalating trend towards the datafication, algorithmization, and platformization of social (inter-)actions and the social organization resulting from these interactions is part of the unprecedented transformative changes that urban society is currently undergoing in light of recent scientific and technological advances, and governance shifts. The digital and computational processes of transforming social (inter-)actions have been made possible by the marked intensification of the datafication of citizens and places as well as urban processes and actions.

At the heart of the Metaverse, as a virtual form of data-driven smart urbanism, is a computational understanding of human users' cognition, emotion, motivation, and behavior that reduces the experience of everyday life to logic and calculative rules and procedures [20]. This computational understanding applies to smart city systems, which epitomize data-driven urbanism informed by urban informatics and urban science that seek to make cities more measurable, manageable, tractable, and controllable, and is the mode of production for smart cities [6]. However, the wide deployment of new networked digital technologies embedded into the fabric of everyday life, together with numerous smartphones apps and a multitude of established social networking, sharing economy, and e-governance platforms in data-driven smart cities, underpin the drive to develop and actualize the Metaverse thanks to platformization. This entails "the penetration of infrastructures, economic processes, and governmental frameworks of digital platforms in different economic sectors and spheres of life, as well as the reorganization of cultural practices and imaginations around these platforms" ([24], p. 1). In this network of agents, information, products, services, resources, and values are exchanged among companies, applications, users, and devices thanks to hyper-connectivity. The widespread diffusion of multiple wireless technologies, especially high-speed 5G networks, will optimize and advance the collection of massive repositories of spatiotemporal data that represent society-wide proxies for human social interactions and activities. This is expected to boom with the introduction of 6G technology, as higher numbers of IoT devices will be able to operate seamlessly on a higher bandwidth [25].

As the magnitude of the data to be generated by the Metaverse will be far greater than that collected from the Internet today, critical concerns are being raised on how Meta and

other big tech companies will use these data and for what purposes and related risks. To put it differently, the soaring deluge of data on social (inter-)action and its analytics using AI algorithms, coupled with the voracious appetite of big tech companies to translate these data into behavioral data and modes of data-driven governance and predictive products, raise a number of ethical and political issues as a result of the logic of surveillance capitalism underlying the Metaverse. For companies, the value of data is not in its presence, but in the ways it can be connected to databases and analytic tools where they can be analyzed, classified, commoditized, and commodified [26].

3. Surveillance Capitalism: Rationales, Risks, Pitfalls, and Gains

As an economic system, capitalism seeks to commodify any new object of economic and political "value" as a condition for its continuation or survival. At the core of surveillance capitalism as a neologism is the commodification of personal data for the purpose of profit-making and power-grabbing, i.e., gaining control over people in opportunistic and unscrupulous ways. Surveillance capitalism refers to the one-sided claiming of the free raw material of private human experience for translation into behavioral data for profit and control [26]. These data are repackaged as prediction products with respect to what people will do now, soon, and in the future that are sold to behavioral futures markets, and offered to government elites. The plethora of ways the repackaged data are repurposed have little, or nothing, to do with what the data generated were originally intended for, in addition to lacking the importance of giving consent to those users that are concerned with the data produced. There is clearly a breach of the data minimization principle in the sense of only generating the data that are relevant and necessary to perform certain tasks and only using these data for the purpose for which they are produced [27].

3.1. Governance and Governmentality in Post-Pandemic Urban Society

Surveillance capitalism was invented by, and pioneered at, Google in 2001 and, later, Meta [28], in the wake of the attacks of 9/11. These events consequently generated much debate about how these big tech companies fundamentally shifted the balance between surveillance and control and privacy and personal autonomy. For example, the control creep that happened post-9/11 was never subsequently rolled back [29,30]. Control creep has occurred since the events of 9/11 across smartphone infrastructures [31], with technologies designed to deliver specific services being enrolled into policing and security apparatuses [32]. With the event of the COVID-19 pandemic, technologies beyond smartphone infrastructure, such as the IoT, AI systems, Big Data ecosystems, edge computing, XR, and blockchain are being subject to control creep, i.e., their original purpose is being extended to perform mass surveillance and data-driven governance in order to normalize the new biopolitical architecture of urban society. Central to the biopolitics [33] of the COVID-19 pandemic is "the close management and control of bodies and their circulation and contact; it is thoroughly spatial in its articulation, regulating public and private spaces, spatial access and behaviour, and producing particular spatialities" ([34], p. 370). However, it seems that history is about to repeat itself with regard to the events of the COVID-19 pandemic and its far-reaching and long-term implications for surveillance society. Many citizens—as well as politicians and policymakers—might believe that the deployment of surveillance technologies is legitimate as long as it helps to limit the spread of the COVID-19 pandemic and thus save lives, irrespective of the concerns it may raise as regards governmentality [34]. As a term combining government and rationality, govenmentality represents the tactics of government that allow it to define and redefine what competencies it entails, or the calculated means that allow it to shape, guide, or affect the conduct of people. It also refers to the "conduct of oneself" or "conduct of conduct" where a sense of self-governance is a guiding force and conduct is beyond leading and directing. Therefore, the state designs systems for defining populations, including management and administration mechanisms and ways of classifying individuals or groups, which make them known and visible by means of their identification, categorization, and control.

However, the COVID-19 pandemic has exacerbated the issues of the increasing involvement of big tech companies in data policies, public trust in data governance, and data privacy risks through the accelerated adoption of digital technologies [35]. It is clear that the movement of big tech companies, such as Meta, Google, Apple, and Microsoft, to help during the COVID-19 pandemic has the effect and motivation of legitimate surveillance capitalism [34], and this is a concern of magnitude as the world prepares to further transition to digital futures. The COVID-19 washing of surveillance capitalism is, in effect, enabled by this legitimation and the invasive harvesting and exploiting of personal (behavioral) data for profit through the laundering of reputations [29,36]. The increasing adoption of the solutionist technologies by both democratic and authoritarian states are boosting the profit of big tech companies and thus the value of their shareholders, providing unparalleled opportunities for them to promote and market their new products, services, and activities pertaining to mass surveillance. Additionally, the digital infrastructures put in place during the COVID-19 pandemic to respond to an urgent crisis is leading to the collection of data at an unprecedented scale, and questions are soon to arise as to what to do with these post-pandemic data, and whether the pandemic-infused digital infrastructures are healthy for humans' quality of life in cities.

The data derived from digital technologies and smartphone apps in smart cities circulate within behavioral markets and are associated with governance corporatization, technocratic reductionism, privacy encroachment, and mind control: social influence to indoctrinate individual and/or group attitudes and beliefs. These have been made possible, and continue to intensify, by the datafication of social (inter-)action and their digital organization within urban society. Datafication is a name for processes of transforming social action into quantified data, allowing companies and government agencies to carry out monitoring and predictive analysis of digital citizens in real time via AI algorithms [37,38]. Surveillance capitalism also focuses on datafying the whole social life by continuously expanding those proportions of it that have the potential for data acquisition and data processing [39]. In particular, we are moving into an era where digital and computing technologies are routinely pervading the very fabric of urban society, paving the way for new forms of control and power grabbing thanks to the global architecture of computer mediation underlying surveillance capitalism and enabled by the escalating trends towards hyper-connectivity, digitalization, datafication, algorithmization, and platformization. The logic of surveillance capitalism depends on this architecture, which "produces a distributed and largely uncontested new expression of power . . . It is constituted by unexpected and often illegible mechanisms of extraction, commodification, and control that effectively exile persons from their own behavior while producing new markets of behavioral prediction and modification" [40].

As a supply chain to surveillance capitalism, Meta has mastered the complexity of the process of gaining and maintaining access to personal data and exploiting these data for its own ends and interests. One of these is legitimizing undemocratic and bad forms of governing urban society, in terms of a lack of transparency and accountability, arbitrary rules and regulations, deception of the governed, and de-democratization. The abrupt digital transformation of urban society—thanks to the COVID-19 pandemic—will make the logic of surveillance capitalism more embedded, automatic, and pervasive in people's everyday lives. While acknowledging that solutionist technologies have numerous benefits, if utilized properly and meaningfully, it is clear that they also reinforce the logic of surveillance capitalism and have profound implications for governmentality (i.e., informal social control, state regulation, calculated means of shaping conduct, etc.), civil liberties, privacy, personal autonomy, and control. For example, contact tracing and movement monitoring apps will, as noted by Aouragh et al. [41]: contribute to determining who can have freedom of choice and decision, co-define who can live and enjoy life, as well as lay out normative conditions for reality, and shaping the perception of the world itself. This opens ground for profound philosophical debates on democracy, freedom, equality, and human rights. Especially, the systems deployed to combat the COVID-19 pandemic will become part of

the "new normal" in monitoring and governing societies—and, hence, will not be turned off after the crisis [30,36]. Since the onset of this crisis and its multifarious consequences have made it clear that its impact will not fade any time soon, and that it will have a long-lasting impact on urban society and the ways of living in it. These will be intimately and permanently interwoven with data-driven governance (e.g., [10,42,43]). Indeed, at the heart of the "new normal" is the intensification of the datafication, algorithmization, and platformization of both socializing, interacting, working, learning, playing, travelling, shopping, and so on, as well as the social organization resulting from these interactions and activities [8]. This epitomizes the core of the Metaverse vision in terms of its ultimate goal to virtualize the ways we live, work, and thrive in urban society, and this will worsen the impacts and risks of digital and computing technologies. This holds true in light of the negative consequences that the social media platforms owned by Meta have had on urban society since the early 2000s due to the deployment of invasive technologies and the implementation of deceptive methods and engagement strategies.

Regardless, surveillance technologies have historically been enrolled into pandemic control and served as solutions up until now [44]. Central to technological solutionism—a deterministic, linear, and overtly rationalistic approach—is the trading of civil liberties for public health and the push of policy by technology rather than vice-versa. This implies that tech-mediated and software-enabled mass surveillance is dictated as the vital means for combating pandemics. But there are no commensurate advantages of using surveillance technologies as long as they cannot deliver the anticipated benefits for public health [36]. Therefore, public health and civil liberties must work in harmony instead of being traded against each other [34] and abused by corporate and government elites by mainstreaming the practices of surveillance capitalism through control and commodification mechanisms. Indeed, for some big tech companies, contributing to the effort to combat the COVID-19 pandemic will act as a gateway to government contracts [30] and monitoring services, as well as to the further privatization of public health data and the further increasing and deepening of data shadows [34] and digital footprints. With respect to the latter, it will be all but impossible for users in the Metaverse to live their everyday life without leaving traces themselves and other traces captured about them due to the pervasiveness of digitally and computationally mediated interactions, communications, and activities, adding to the increasing use of unique identifiers to access a myriad of virtual services.

In the era of digitalization, governments turn to solutionist technologies for—questionably —pressing policy issues when it comes to crises, and those related to the COVID-19 pandemic are no exception. Crises and pandemics—especially if engineered—mean intensifying and cementing surveillance practices by big tech companies and potentially legitimating tyranny by democratic states through eroding civil liberties and privacy. In particular, unjustifiably violating people's privacy is a byproduct of surveillance that is too often criticized by civil society organizations and that has been exacerbated by the COVID-19 pandemic [8]. Hence, it is crucially important to document the ways in which a new surveillance regime is being established through the merger of surveillance capitalism and government control through the technologies rolled out in the wake of the COVID-19 pandemic and developed by big tech companies. With the Metaverse, the capabilities of surveillance technologies will be greatly sharpened and extended beyond the common methods (e.g., account numbers, credit-card numbers, transaction records, emails, addresses, phone call details, smart card ID) to include smartphone apps, faces, biometric wearables, smart helmets, smart watches, Brain–Computer Interfaces (BCI), BioID, digital ID, drones, and predictive analytics [8]. The Metaverse will be able to detect and constantly monitor what people are doing, with whom they are talking, and where they go, and also to connect and search isolated available databases containing personal and sensitive information. These practices, which are designed to rescript how people live their lives, have long-term implications for not only privacy, but also governmentality and civil liberties. The fine-grained mass tracking of movement and proximity, and the monitoring and collection of online data—thanks to geosurveillance and dataveillance—will enable tighter forms of control and will have

frightening effects on democracy and civil liberties. Such a pathway is legitimized because "authoritarianism—for the 'right' reasons—starts looking tolerable, even good, because it looks like the only option" [30].

The Metaverse is associated with democratic decay, and, in it, the rules and regulations will be entirely different due to the model of surveillance capitalism it embodies. As argued by Zuboff [28], "dispossession by surveillance" challenges the political and psychological bases of self-determination, as it concentrates rights in the surveillance regime, describing this as a "coup from above." Self-determination is about people's choices as a self-motivated and self-determined human behavior in the absence of external influences [45]. To further complicate matters, every virtual world of the numerous ones that will be built in the Metaverse is expected to have its separate rules to govern the behaviors and activities of users [3]. This raises critical questions as to how digital urban societies will thrive, the new cultures that may emerge, and the governance structures that these cultures will require. In particular, unfairness is a critical issue with respect to the guidelines and principles that will be applied in the Metaverse to behaviorally profile and socially sort users in the virtual world. The Metaverse should take into account the algorithmic fairness as the core value of its designs [46] and hence maintain the procedural justices [47] to undertake governance roles, which "requires a high degree of transparency to the users and outcome control mechanisms" [3]. This though runs counter to the foundational vision of the Metaverse and what its underlying algorithmic techniques and engagement strategies are primarily aimed at in the constantly surveilled urban society that Meta has hugely invested in and significantly contributed to legitimating since the early 2000s. Regardless, algorithmic governance involves unevenness and inequity, which reproduce data justice issues [48,49] across different demographics [50,51] with potentially harmful consequences.

Ominously, the Metaverse will—by the very nature of the underlying technologies of its ecosystem application—invasively harvest a colossal amount of biometric and online data about individual users' identities, bodies, minds, histories, profiles, preferences, interactions, transactions, and activities. In particular, biodata raise a serious concern because at their very core lies the ethical issues of privacy, control, manipulation, and health [20]. However, surveillance capitalism involves dataveillance, geosurveillance, and anticipatory governance as a means to advance the hidden agenda of the ruling corporate and governmental elites. This relates to corporatism, the merger of the corporate power and the state power. The logic of public–private partnerships and the fusion between the corporatist and the state entails that there should be an alliance between the interest of global corporations and those of the state. The way in which Western societies have been steered for several decades reflects a fragmentation and transfer of power and responsibility from governments and public bodies of representative democracies to corporate interests and NGOs [52]. Western societies have outsourced democratic resilience to big tech companies and hence increased the power of the powerful elites, raising concerns over accountability, representation, and transparency. The paradox lies in that democracies become less resilient as their institutions become weak and the judicial constraints on their executive authorities become absent. This is due to the fact that the rules and regulations become concentrated in the surveillance regime of capitalists and elites who set the global agenda and curtail the opportunity for democratic engagement and supervision, i.e., undermining the power of an established system. As supported by Boese et al. [53], as "a two-stage process where democracies avoid democratic declines altogether or avert democratic breakdown ... , democratic resilience has become substantially weaker ... and substantial declines in democratic practices have occurred since 1993, leading to the unprecedented breakdown of democratic regimes". This has paved the way for global corporatists to take over the power of governments in democratic societies by means of constant surveillance and mass control. Capitalism has shifted the balance of power from nation-states towards large corporations, employing the surveillance logic of capitalists [54]. With reference to social media, Fuchs [55] found that the surveillance capitalism fuses with the surveillance state. This issue is further complicated by hidden collaborative arrangements with state security

apparatuses [26]. As a hegemonic discourse, the relationship between the Metaverse, the surveillance capitalism, and the surveillance state "is constructed in the light of culturally specific, historically contingent, and episteme conditioned conceptions about the social, political, institutional, economic, and technological changes" [56].

However, the Metaverse may, extrapolating from the past, employ many new deceptive methods to impede the ability of people to grasp their ethical and political implications, as well as to keep them unaware at best and ignorant at worst of how they are being governed and of the kind of arrangements that are intricately interwoven with governmental apparatuses and their techniques. As the Metaverse is made for corporations and governments—not for people and by people—it will rather engage in building the backbone for authoritarian regimes in a new disguise with respect to the blind submission of citizens to authority in urban society and the execution of rules by corporate and government elites. This situation is compounded by the fact that surveillance capitalism has gone beyond the surveillance-based ecosystems of big tech companies to include those of every economic sector thanks to the COVID-19 pandemic. This connects well with techno-fascism, which employs digital media and advanced technology to attain its ends, and where only technocratic elites have political rights. Routinizing new forms of social and spatial sorting as a result of the new type of management enabled by the technologies being implemented during the COVID-19 pandemic has "the potential to permanently shift the nature of governmentality and to also act as a pathway towards authoritarian forms of governance where technology is used to actively impose the will of the state onto citizens" [34]. According to UN privacy chief Joseph Cannataci, who warns against the long-lasting theft of freedoms in the middle of COVID-19 surveillance, "Dictatorships and authoritarian societies often start in the face of a threat . . . that is why it is important to be vigilant today and not give away all our freedoms" [57]. Dystopias portray surveillance societies with unlimited control and dictatorship—absolute power concentrated in the hands of a ruler. We can see a parallel in post-pandemic societies with regard to the massive use of surveillance technologies by many governments to interfere and limit the private life of citizens. The long-term impacts of digital technologies and the use of data tools for pandemic control have potentially detrimental and irreversible impacts on society in the long [35].

3.2. The Financial Gains and Market Capitalization of the Metaverse

Surveillance capitalism works by monitoring people's behaviors and movements online and in the physical world to capture their data for commoditization, monetization, and trading. The unethical aspect of surveillance capitalism lies in harvesting and exploiting users' personal information for financial gains by transforming the experience of human users into behavioral data, and by mining their data to control and predict their behavior. In this light, it is important to highlight the economic implications of the Metaverse. This mega project is attracting considerable investment, funding, and public attention and thereby generating numerous R&D projects, programs, and consortia across a plethora of business and industry domains. It is pushing the global market towards unparalleled profitable paths. Meta and other platform providers, as well as major corporations, have begun investing billions of dollars to develop the Metaverse given the rising prospect that it will greatly impact urban society over the next decade. In relation to the Extended Reality (XR), the global AR, VR, and MR market was already forecast to reach USD 30.7 billion in 2021, rising to close to USD 300 billion by 2024 [58]. As echoed by Nordor Intelligence [59], it was estimated that the XR market was valued between USD 26.05 and USD 33 billion. It is also anticipated that, following the current interests in XR, the consumer market would grow to approximately USD 125.2 billion by 2026 [60]. The number of worldwide shipments of XR headsets is forecasted to increase to 105 million by 2025, and VR and AR headsets are expected to transform the way users experience media and social networking, as well as software applications [58]. Only AR capacities may prompt an increased demand for AR glasses, as users seek to maximize their virtual experience. There will be an estimated

1.7 billion mobile AR users worldwide by 2024, and there is an estimated 1.1 billion mobile AR users worldwide in 2022 [58]. As a result, the market value for AR glasses is projected to grow from the current estimated value of USD 7 billion to a high of USD 157 billion by 2030 [61]. Already, it is conceded that thousands of billions of dollars have been spent by consumers of virtual digital products, especially in the gaming world, where users purchase different digital accessories for their online avatars. According to a recent survey, 65% of respondents are willing to spend up to USD 1000 to acquire advanced VR gear, such as a haptic suit, gloves, and shoes [22]. Figure 1 illustrates, based on recent statistics, the global market capitalization of the Metaverse, Meta, and gaming 2021 [22]. In addition, as a digital twin of work in the physical world, the Metaverse platform will promote all kinds of brands. Given the rich diversity of technologies featured in the Metaverse and the broad variety of potential products and applications, it is believed that the economic prospects of the Metaverse will eventually justify current and future investment.
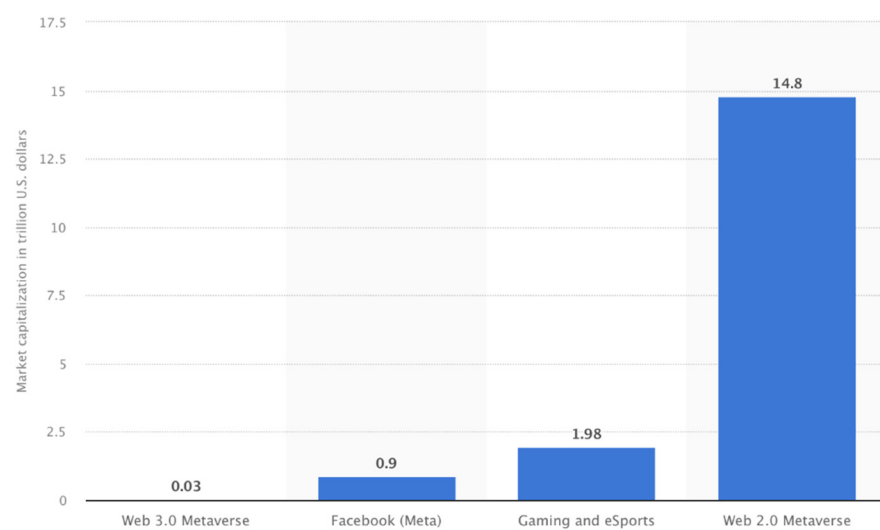
Figure 1. Market capitalization of the Metaverse, Meta, and gaming worldwide as of October 2021 ([22]).

In terms of surveillance capitalism, trading personal data repackaged in behavioral products and data services is a multi-billion dollar industry consisting of a diverse ecosystem of different types of specialist companies as data brokers that are focused on specific markets [6]. These companies offer services that are used to regulate, control, and govern individuals, as well as the various systems and platforms with which they interact [13]. The underlying argument is that the Metaverse epitomizes the market-driven process of surveillance capitalism in terms of trading user personal information by translating it into behavioral data, relying on the mass surveillance of the Internet and thus scrutinizing online interactions, communications, and activities in order to provide virtual services to users. Control and decision making are already left in the hands of AI algorithms in accordance with criteria intended mainly for legitimating and cementing surveillance capitalism and thus increasing control and abusing power, leading to corrosive consequences. The increasingly hyperconnected, datafied, algorithmized, and platformized urban society benefits the more fortunate and powerful and punishes the unfortunate and weak (e.g., [8,62]). This requires deep reflection on the ethical implications of the digital transformation of urban society [63]. Expanding the global market for new technological products and services often ignores their wider impacts on people as consumers and supports never-realized noble ideas and goals. Consuming the Metaverse technologies, which is presented as a form of citizen participation, must be approached carefully because big tech companies as centralized structures often have hidden economic and political motives that they are driven by. As argued by Viitanen and Kingsto [15], smart city systems represent "a digital marketplace

where citizen-consumers' participation is increasingly involuntary and the hegemony of global technology firms is inflated . . . , [resulting in] a digital consumer experience that has inherent biases and leaves parts of the city and its population unaccounted for".

4. Conclusions

The Metaverse raises serious concerns over the risks and impacts of its underlying technologies with regard to the core values of urban society. This viewpoint paper has highlighted how and why the practices of the post-pandemic governance of urban society are bound to be undemocratic and unethical. The how relates to the global architecture of the computer mediation of the Metaverse that underpins the logic of surveillance capitalism in terms of the synergic operation of hyper-connectivity, digitalization, datafication, algorithmization, and platformization as a set of systems, devices, things, processes, and techniques. The why pertains to the core purpose of surveillance capitalism that is enacted through its control and commodification mechanisms, and that increases the power of the powerful (corporate and government elites) through eroding democracy, undermining privacy and personal autonomy, and evaporating civil liberties. The political and ethical principles designed to protect the dignity of human beings in urban society ought not to be traded off against the empty promises of the benefits that individuals may have in exchange for allowing big tech companies to invasively harvest and exploit their personal data. This is only designed to shape, control, and predict human user behavior to produce docile, submissive, compliant bodies. The technocratic, algorithmic, automated nature of technologies can shift the governmental logic from surveillance and discipline to capture and control [64]. The promotion and use of invasive technologies in the age of surveillance capitalism trump concerns over human and civil rights, and are often packaged as being a means to care for the public health of citizens. Social media platforms have fanatically supported the idea that citizens should give up their rights for the sake of public health. In this vein, digital societies are rushing into and accepting all kinds of invasive technologies with immediate and long-term consequences concerning surveillance capitalism—with mostly collective disadvantages in return.

In addition, the transformation of personal data into objects of trade has been a subject of much debate over whether anything should be intended for exchange, predicated on the assumption that there are things that ought not to be treated as commodities, such as data on human experience, private life, social life, health, and so forth. Regardless, the infrastructures, platforms, systems, and applications providing data-driven solutions have become a digital marketplace where the supremacy and dominance of big tech companies are inflated and the inherent socio-economic biases are exacerbated, leaving citizens unaccounted for. Still, it is far from clear how to build upon existing and emergent socio-economic demands and how to make money out of the Metaverse. However, the Metaverse continues to promote empty promises in an attempt to figure out new ways to cater for increased demands from the youth group of urban society to make more money as the real world's resources are dwindling.

The hope seems to be lost with regard to the potential of trusting digital technologies and using them responsibly. In particular, most of the policies, regulations, legislations, and auditing mechanisms created and established in the wake of the COVID-19 pandemic are of a destructive nature and directed towards stripping away people from their natural and constitutional rights. Large corporations and organizations are pushing for particular behavioral opportunities for the public because they are armed with technological and political power that outsmart people through forces beyond their control thanks to constant surveillance.

The insights provided in this viewpoint paper remain valid in light of the pernicious effects inflicted by the social media platforms on urban society over the last two decades, and which will be exacerbated with the Metaverse. As such, they are for policy makers to better understand the imminent political and ethical risks posed by the Metaverse, and to take a less naïve view about them in order to create an open, free, fair, and healthy urban

society. However, one might wonder if it is still sensible and prudent to consider plans for designing meaningful policies and implementing regulations that benefit all people given the decline in democratic regimes and the erosion of societal values witnessed globally in the aftermath of the engineered COVID-19 pandemic.

References

1. Bosworth, A.; Nick, C. Building the Metaverse Responsibly. 2021. Available online: https://about.fb.com/news/2021/09/building-the-metaverse-responsibly (accessed on 23 February 2022).
2. Hemmati, M. The Metaverse: An Urban Revolution Effect of the Metaverse on the Perceptions of Urban Audience Tourism of Culture. *Tour. Cult.* **2022**, *2*, 53–60. [CrossRef]
3. Lee, L.H.; Braud, T.; Zhou, P.; Wang, L.; Xu, D.; Lin, Z.; Kumar, A.; Bermejo, C.; Hui, P. All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda. *arXiv* **2021**, arXiv:2110.05352.
4. Bina, O.; Inch, A.; Pereira, L. Beyond techno-utopia and its discontents: On the role of utopianism and speculative fiction in shaping alternatives to the smart city imaginary. *Futures* **2020**, *115*, 102475. [CrossRef]
5. Bibri, S.; Krogstie, J. Data-Driven Smart Sustainable Cities of the Future: A Novel Model of Urbanism and its Core Dimensions, Strategies, and Solutions. *J. Futures Stud.* **2020**, *25*, 77–94. [CrossRef]
6. Kitchin, R. The ethics of smart cities and urban science. Philosophical Transactions of the Royal Society A: Mathematical. *Phys. Eng. Sci.* **2016**, *374*, 20160115. [CrossRef]
7. Nikitin, K.; Lantsev, N.; Nugaev, A.; Yakovleva, A. *Data-Driven Cities: From Concept to Applied Solutions*; Pricewater-houseCoopers (PwC): London, UK, 2016. Available online: http://docplayer.net/50140321-From-concept-to-applied-solutions-data-driven-cities.html (accessed on 25 March 2020).
8. Bibri, S.E.; Allam, Z. The Metaverse as a Virtual Form of Data-Driven Smart Cities: The Ethics of the Hyper-connectivity, Datafication, Algorithmization, and Platformization of Urban Society. *Comput. Urban Sci.* **2022**, *2*, 22. [CrossRef]
9. Bridge, G. Urbanism. In *International Encyclopedia of Human Geography*; Kitchin, R., Thriftedited, N., Eds.; Elsevier: Oxford, UK, 2009; pp. 106–111.
10. Bibri, S.E. The Social Shaping of the Metaverse as an Alternative to the Imaginaries of Data-Driven Smart Cities: A Study in Science, Technology, and Society. *Smart Cities* **2022**, *5*, 832–874. [CrossRef]
11. Gregory, D.; Johnston, R.; Pratt, G. *Dictionary of Human Geography*; Wiley-Blackwell: Hoboken, NJ, USA, 2009.
12. Harvey, D. *Social Justice and the City*; Edward Arnold: London, UK, 2009.
13. Kitchin, R. *The Data Revolution, Big Data, Data Infrastructure and Their Consequences*; Sage: California, CA, USA, 2014; p. 200. ISBN 978-1-4462-8747-7.
14. Allam, Z.; Ayyoob, S.; Bibri, S.E.; Jones, D.S.; Krogstie, J. The Metaverse as a Virtual Form of Smart Cities: Opportunities and Challenges for Environmental, Economic, and Social Sustainability in Urban Futures. *Smart Cities* **2022**, *5*, 771–801. [CrossRef]
15. Viitanen, J.; Kingston, R. Smart cities and green growth: Outsourcing democratic and environmental resilience to the global technology sector. *Environ. Plan. A* **2015**, *46*, 803–819. [CrossRef]
16. Bibri, S.E. Data-driven smart sustainable cities of the future: An evidence synthesis approach to a comprehensive state-of-the-art literature review. *Sustain. Futures* **2021**, *3*, 100047. [CrossRef]
17. Verrest, H.; Pfeffer, K. Elaborating the urbanism in smart urbanism: Distilling relevant dimensions for a comprehensive analysis of Smart City approaches. *Inf. Commun. Soc.* **2019**, *22*, 1328–1342. [CrossRef]
18. Marvin, S.; Luque-Ayala, A.; McFarlane, C. (Eds.) *Smart Urbanism: Utopian Vision or False Dawn*; Routledge: London, UK, 2015.
19. Bibri, S.E. Data-driven smart eco-cities and sustainable integrated districts: A best-evidence synthesis approach to an extensive literature review. *Eur. J. Futures Res.* **2021**, *9*, 16. [CrossRef]
20. Bibri, S.E.; Allam, Z.; Krogstie, J. The Metaverse as a Virtual Form of Data-Driven Smart Urbanism: Platformization and its Underlying Processes, Institutional Dimensions, and Disruptive Impacts. *Comput. Urban Sci.* **2022**, *2*, 24. [CrossRef]
21. Falchuk, B.; Loeb, S.; Neff, R. The social metaverse: Battle for privacy. *IEEE Technol. Soc. Mag.* **2018**, *37*, 52–61. [CrossRef]
22. Johnson, J. *Metaverse—Statistics & Facts*; Statista: Hamburg, Germany, 2022. Available online: https://www.statista.com/topics/8652/metaverse/ (accessed on 25 February 2022).

23. Rosenberg, L. Regulation of the Metaverse: A Roadmap. In Proceedings of the 6th International Conference on Virtual and Augmented Reality Simulations (ICVARS 2022), Brisbane, Australia, 1 November 2022.

24. Poell, T.; Nieborg, D.; Van Dijck, J. Platformisation. *Internet Policy Rev.* **2019**, *8*, 1–13. [CrossRef]

25. Allam, Z.; Jones, D.S. Future (post-COVID) digital, smart and sustainable cities in the wake of 6G: Digital twins, immersive realities and new urban economies. *Land Use Policy* **2021**, *101*, 105201. [CrossRef]

26. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; Profile Books: London, UK, 2019.

27. OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980. Available online: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed on 10 October 2015).

28. Zuboff, S. The Secrets of Surveillance Capitalism. 2016. Available online: https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html?printPagedArticle=true (accessed on 12 March 2022).

29. McDonald, S. *The Digital Response to the Outbreak of COVID-19*; Centre for International Governance Innovation: Waterloo, ON, Canada, 2020. Available online: https://www.cigionline.org/articles/digital-response-outbreak-covid-19 (accessed on 10 April 2022).

30. Sadowski, J. The Authoritarian Trade-Off: Exchanging Privacy Rights for Public Health is a False Compromise. *Real Life gazine*. 13 April 2020. Available online: https://reallifemag.com/the-authoritarian-trade-off/ (accessed on 17 June 2021).

31. Innes, M. Control Creep. *Sociol. Res. Online* **2001**, *6*, 13–18. Available online: http://www.socresonline.org.uk/6/3/innes.html (accessed on 15 July 2021). [CrossRef]

32. Kitchin, R.; Dodge, M. *Code/Space: Software and Everyday Life*; MIT Press: Cambridge, MA, USA, 2011.

33. Foucault, M. *Discipline and Punish: The Birth of the Prison*; Pantheon Books: New York, NY, USA, 1977.

34. Kitchin, R. Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space Polity* **2020**, *24*, 362–381. [CrossRef]

35. Li, V.Q.; Ma, L.; Wu, X. COVID-19, policy change, and post-pandemic data governance: A case analysis of contact tracing applications in East Asia. *Policy Soc.* **2016**, *41*, 1–14. [CrossRef]

36. Stanley, J.; Granick, J.S. *The Limits of Location Tracking in an Epidemic*; ACLU: New York, NY, USA, 2020. Available online: https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf (accessed on 10 April 2022).

37. Van Dijck, J. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveill. Soc.* **2014**, *12*, 197–208. [CrossRef]

38. Van Dijck, J. La Cultura de la Conectividad. In *Una Historia Crítica de las Redes Sociales*; Siglo XXI Editores: Buenos Aires, Argentina, 2016.

39. Couldry, N. The Price of Connection: "Surveillance Capitalism". 2016. Available online: https://theconversation.com/the-price-of-connection-surveillance-capitalism-6412 (accessed on 14 July 2017).

40. Zuboff, S. 1015 Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *J. Inf. Technol.* **2015**, *30*, 75–89. [CrossRef]

41. Aouragh, M.; Pritchard, H.; Snelting, F. *The Long Tail of Contact Tracing. D3PT (Decentralized Privacy-Preserving Proximity Tracing)*; GitHub: San Francisco, CA, USA, 2020. Available online: https://github.com/DP-3T/documents/issues/118 (accessed on 12 December 2021).

42. Allam, Z. *Surveying the COVID-19 Pandemic and Its Implications: Urban Health, Data Technology and Political Economy*; Elsevier: Amsterdam, The Netherlands, 2020.

43. Allam, Z.; Jones, D.S. Pandemic stricken cities on lockdown. Where are our planning and design professionals [now, then and into the future]? *Land Use Policy* **2020**, *97*, 104805. [CrossRef]

44. French, M.; Monahan, T. Dis-Ease Surveillance: How Might Surveillance Studies Address COVID-19? *Surveill. Stud.* **2020**, *18*, 1–11. Available online: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13985 (accessed on 11 November 2021). [CrossRef]

45. Ryan, R.M.; Deci, E.L. *Self-Determination Theory: Basic Psychological Needs in Motivation, Development, and Wellness*; Guilford Publishing: New York, NY, USA, 2017.

46. Woodruff, A.; Fox, S.E.; Rousso-Schindler, S.; Warshaw, J. A qualitative exploration of perceptions of algorithmic fairness. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18, Montreal, QC, Canada, 21–26 April 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–14.

47. Lee, M.K.; Jain, A.; Cha, H.J.; Ojha, S.; Kusbit, D. Procedural justice in algorithmic fairness: Leveraging transparency and outcome control for fair algorithmic mediation. *Proc. ACM Hum.-Comput. Interact.* **2019**, *3*, 1–26. [CrossRef]

48. Dencik, L.; Hintz, A.; Cable, J. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data Soc.* **2016**, *3*, 2053951716679678. [CrossRef]

49. Taylor, L. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data Soc.* **2017**, *4*, 2053951717736335. [CrossRef]

50. Benjamin, R. *Race after Technology: Abolitionist Tools for the New Jim Code*; Polity Books: Cambridge, UK, 2019.

51. Noble, S.U. *Algorithms of Oppression: How Search Engines Reinforce Racism*; New York University Press: New York, NY, USA, 2018.

52. Kramers, A.; Wangel, J.; Höjer, M. Governing the smart sustainable city: The case of the Stockholm Royal Seaport. In Proceedings of the ICT for Sustainability, Amsterdam, The Netherlands, 29 August–1 September 2016; Atlantis Press: Amsterdam, The Netherlands, 2016; Volume 46, pp. 99–108.

53. Boese, V.A.; Edgell, A.B.; Hellmeier, S.; Maerz, S.F.; Lindberg, S.I. How democracies prevail: Democratic resilience as a two-stage process. *Democratization* **2021**, *28*, 885–907. [CrossRef]

54. Galič, M.; Timan, T.; Koops, B.J. Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philos. Technol.* **2016**, *30*, 9–37. [CrossRef]

55. Fuchs, C. *Social Media: A Critical Introduction*; SAGE Publications: London, UK, 2017.

56. Bibri, S.E. The Potential Catalytic Role of Green Entrepreneurship—Technological Eco–innovations and Ecopreneurs' Acts—in the Structural Transformation to a Low–Carbon or Green Economy: A Discursive Investigation. Master's Thesis, Lund University, Lund, Sweden, 2014.

57. Gregory, A. Dictatorships often Start in the Face of a Threat: UN Privacy Chief Warns against Long-Lasting Theft of Freedoms Amid Coronavirus Surveillance. Independent. 2020. Available online: https://www.independent.co.uk/news/world/coronavirus-lockdown-surveillance-tracking-dictatorship-authoritarian-united-nations-privacy-a9438561.html (accessed on 25 February 2022).

58. Thomas, A. Augmented Reality (AR) and Virtual Reality (VR) Market Size Worldwide 2016–2024. 2021. Available online: https://www.statista.com/statistics/591181/global-augmented-virtual-reality-market-size/ (accessed on 25 February 2022).

59. Nordor Intelligence. *Extended Reality (XR) Market—Growth, Trends, COVID-19 Impact, and Forecast (2021–2026)*; Mordor Intelligence: Hyderabad, India, 2021. Available online: https://www.mordorintelligence.com/industry-reports/extended-reality-xr-market (accessed on 1 December 2021).

60. Markets and Markets. Extended Reality Market with COVID-19 Impact Analysis by Technology (AR, VR, MR), Application (Consumer, Commercial, Enterprises, Healthcare, Aerospace and Defense), Offering, Device Type, and Region (North America, Europe, APAC)—Global Forecast to 2026. Available online: https://www.marketsandmarkets.com/Market-Reports/extended-reality-market-147143592.html (accessed on 1 December 2021).

61. Apple World. *Augmented Reality Market Projected to be Worth $7 Billion by 2030*; Apple World: Sydney, NSW, Australia, 2021. Available online: https://www.appleworld.today/2021/11/16/augmented-reality-market-projected-to-be-worth-7-billion-by-2030/ (accessed on 2 December 2021).

62. O'Neil, C. *Weapons of Math Destruction How Big Data Increases Inequality and Threatens Democracy*; Crown Publisher: New York, NY, USA, 2016.

63. Calvo, P. The ethics of Smart City (EoSC): Moral implications of hyperconnectivity, algorithmization and the datafication of urban digital society. *Ethics Inf. Technol.* **2020**, *22*, 141–149. [CrossRef]

64. Deleuze, G. Postscript on the societies of control. *October* **1992**, *59*, 3–7.