International Journal of Communication 16(2022), 1–18 1932–8036/20220005

Imagining 5G Networks: Infrastructure and Public Accountability

ROBIN MANSELL
JEAN-CHRISTOPHE PLANTIN[1]
London School of Economics and Political Science, UK

This study explores the social imaginaries influencing choices about the architectural design and standards for the 5G mobile network to identify how the network level of the communication infrastructure is implicated in the commercial datafication process. We focus on ambitions to establish global market leadership in the provision of the 5G infrastructure. Based on a multimethod analysis of documentation, press coverage, and a case study of 5G's radio access network standardization, the analysis provides insight into contradictions within a dominant digital innovation social imaginary that privileges national or regional economic 5G strategies and externalizes risks and threats around 5G networks to foreign actors (mainly China). It also shows how public values, including privacy and freedom from surveillance, as well as transparent public accountability, characteristics of an alternative social imaginary of digital innovation, are suppressed in the process of materializing a new communication infrastructure.

Keywords: artificial intelligence, datafication, 5G, mobile communication, standards, social imaginary

Mobile communication networks have become a critical infrastructure in most people's lives. The arrival of a fifth generation (5G) network is signaled by debate about who should build it and how it should be used. 5G-enabled handsets are being marketed to users and the potential benefits of 5G-powered applications such as the Internet-of-Things (IoT), augmented virtual reality, and autonomous cars are being widely promoted. Expectations about a new network architecture matter because they influence whether citizens' fundamental rights will be protected in a future involving the massive collection and processing of data, which 5G is capable of delivering.

Robin Mansell: r.e.mansell@lse.ac.uk
Jean-Christophe Plantin: j.plantin1@lse.ac.uk
Date submitted: 2021-05-24

[1] We gratefully acknowledge the contributions to the content analysis reported in this study by master's students in the Department of Media and Communications at LSE and the support for this research by the department's research fund. We are also grateful to anonymous referees whose comments were very helpful in prompting us to clarify our argument. Any errors or omissions remain our responsibility.

When there is a risk that citizens' fundamental rights can be harmed by the underlying "root," or networking, level of the communication infrastructure (Plantin, Lagoze, Edwards, & Sandvig, 2018), this generally receives less attention than do harms linked to what Van Dijck has described with the metaphor of the "trunk" (i.e., digital platform) or "branch" (i.e., software applications) levels of the infrastructure (Van Dijck, 2020). Our examination of the 5G mobile communication infrastructure emphasizes the need to address public accountability issues at the "root" level of the communication infrastructure, since it is a key building block for digital platforms and AI-enabled services. In this study, we examine imaginaries or expectations concerning the 5G infrastructure as they are represented in policy, industry and standards documents, and in the press. Our investigation is based on a document analysis, a content analysis of 5G media coverage, and a case study of an important component of the 5G infrastructure—the OpenRAN (Radio Access Network). Our aim is to explore how expectations concerning digital innovation become complicated by conflicting values and aspirations at the 5G "root" level of communication infrastructure innovation in the United Kingdom, the United States, and the European Union.

In the next section, we present our theoretical framing of expectations of digital innovation, which elaborates on Taylor's (2002, 2007) notion of the "social imaginary" and our multimethod approach. We then offer a profile of 5G innovation based on a review of 5G-related documentation, highlighting values, and aspirations and how claims that are made about 5G tend to render invisible the public values associated with critical perspectives on the rise of a data economy. In the fourth section, we discuss how the British press has positioned 5G with particular attention to what these media representations of 5G issues tell us about the influence of a dominant digital innovation social imaginary and the tensions among the values it embraces. Section five presents a case study of a component of the 5G infrastructure—the RAN—to illustrate the role that standardization plays in embedding values consistent with a dominant social imaginary, while creating possibilities for pursuing geopolitical objectives and corporate aspirations for 5G market leadership. In section six, we reflect on how a splintering of 5G standardization activity favors the interests of Western actors, while concealing values associated with an alternative social imaginary of digital innovation that might be more likely to protect citizens from privacy infringements and surveillance. In the concluding section, we argue that analysis of a dominant digital innovation social imaginary at the infrastructure "root" level—as illustrated by 5G innovation—not only draws attention to its internal contradictions but also to how it operates to suppress alternative 5G materializations.

The Social Imaginary and Technological Innovation

The social imaginary is understood by political philosopher Charles Taylor (2007) as "the deeper normative notions and images" invoked by the way "things go on among people" (p. 117); "it is what enables, through making sense of, the practices of a society" (Taylor, 2002, p. 91). For Taylor (2002), a social imaginary is comprised of values that achieve a certain legitimacy in society (Calhoun, 2002; Mansell, 2012). He argues that actors in society tend to share a common set of values in a given historical period that influence their expectations and aspirations. This does not mean, however, that values held by a given set of actors will be well aligned with each other or that a social imaginary is uncontested, unchanging, or unnuanced by differing priorities accorded to political or economic values. In this framing, social imaginaries are subject to contestation as norms and values change. In our context, social imaginaries concerning digital innovation, and 5G in particular, are understood to shape expectations about markets, infrastructure

designs, and architectures, making some characteristics appear inevitable and downplaying alternatives (Mansell & Steinmueller, 2020, 2022).[2]

In a context of contemporary digital innovation, a social imaginary that predominates in societies around the world is one that privileges data-driven economic growth, guided by technological innovation strategies in a globally (idealized) competitive marketplace (Mansell, 2012; Mansell & Steinmueller, 2022; Meng, 2021; Moore & Tambini, 2022). The way "things go on among people" is imagined to be through company, country, or region participation in a competitive technology-innovation race, with success defined by healthy profit margins, favorable trade balances, and strong economic growth indicators in the digital marketplace. Informed by neoliberal values and a narrow focus on innovation in business models and technology designs and architectures, this social imaginary tends to externalize risks and harms to citizens associated with the innovation process (Mansell & Steinmueller, 2020).

This imaginary of digital innovation is pervasive, and it operates to minimize or make invisible potential risks to citizens' rights to privacy, their freedoms from surveillance, or the harms associated with discrimination because of the development of commercial datafication networks (Mansell, 2012; Mansell & Steinmueller, 2022; Meng, 2021; Powell, 2021). When this social imaginary informs decisions, it is often taken for granted that commercial values and aspirations will be balanced with public values through the technology designs that are brought to market and, additionally, that concerns about whether this balance is being (or will be) achieved should not slow the pace of innovation.

An alternative social imaginary of digital innovation is signaled by critics of digital innovation strategies who argue that prevailing innovation strategies exacerbate datafication and surveillance practices with negative implications for the protection of citizens' rights (Couldry & Mejias, 2019; Mansell & Steinmueller, 2020; Van Dijck, Poell, & De Waal, 2018; Werbach, 2022; Zuboff, 2019). From this critical perspective, under capitalism, most, if not all, instances of digital innovation involve choices about standards, technology designs, network architectures, and policies that amplify the risk that protections of citizens' fundamental rights to privacy, freedoms from surveillance, and data-related discriminations will be neglected. This alternative social imaginary of digital innovation suggests the need for strengthened accountability mechanisms and enhanced respect for public values in relation to uses of data and algorithms, artificial intelligence (AI), and machine learning generally (Crawford, 2021; Gillespie, 2017; Van Dijck et al., 2018), as well as in relation to harms arising from data capture and automated decision making in multiple sectors, such as retail (Turow, 2017), banking (Pasquale, 2015), online advertising (Noble, 2018), policing (Brayne & Christin, 2020), and social services (Eubanks, 2018).

Social imaginaries, as explained by Taylor (2002, 2007), are unstable because of changing configurations of values and beliefs. Thus, it is an empirical question as to how internal contradictions within

[2] A social imaginary in our theoretical framing is not synonymous with a sociotechnical imaginary as developed in the science and technology studies tradition. A social imaginary in our context concerns values and normative expectations but does not itself indicate how these will be articulated when decisions are taken. It is open to empirical exploration using various methods and typically is applied at the institutional or meso-analytical level.

a dominant social imaginary of digital innovation operate and the extent to which an alternative social imaginary—that is, an imaginary embracing and elevating respect for public values (responsiveness to democratic values, privacy protection, individual autonomy in decision making)—is visible and has a potential to gain traction as the innovation process proceeds. Over time, as Taylor's (2002, 2007) accounts of the history of social imaginaries emphasize, struggles occur among actors adhering to varying combinations of beliefs and values. Although dominant and alternative social imaginaries may have common features insofar as progressive incorporation of digital technologies into societies is encouraged, they differ substantially with where the power should reside to make choices about characteristics of an all-encompassing technologically mediated environment and which interests it should principally serve. In the dominant imaginary, power is located with an abstract notion of a capitalist market (and its individual agents); in alternative imaginaries, power is located with the choices of both autonomous individuals and their collective institutions.

The social imaginary is a high-level construct, but it is possible to gain some purchase on how values are being materialized in the case of digital innovation by focusing on a particular component of the "root" of the infrastructure—in our case, of the 5G infrastructure. The features of social imaginaries that are collectively held and, on occasion, resisted, can be expected to be present in the practices of actors engaged in promoting and developing the 5G infrastructure and in how they represent their values and aspirations about those practices, whether these representations appear in the media, state policies, and corporate reports, or in documentation of standardization activities. Our multimethod approach to gain insight into the instantiation of these social imaginaries and their consequences was initially based on a review of some 90 publicly available documents (legislation, policies, corporate reports, standards documentation) on the development of 5G network services in the United Kingdom, the United States, and the European Union from 2016 to 2020. This documentation was reviewed to identify key claims and disputes about the development of the 5G network infrastructure. Having developed profiles of how 5G is portrayed, we sought evidence of claims about 5G in the press. A quantitative content analysis of reporting of 5G issues in the United Kingdom was undertaken (Mansell & Plantin, 2020), focusing on 2017 to 2020, a period of heightened controversy over the involvement of Chinese companies in Western infrastructure development and about 5G's implications for data security. A third component of our investigation was a case study analysis of an important component of the 5G network development—the OpenRAN. This involved a review of websites and standards documents related to the design and architecture of this component of 5G, focusing on technical standardization as a site of contestation over the values that should inform the materialization of a technology.

Our multimethod approach was intended to reveal some of the diverse features of social imaginaries of digital innovation and to provide insight into how a dominant imaginary is being materialized as well as into the scope for favoring values consistent with an alternative social imaginary.

Government and Industry 5G Expectations

We start by profiling 5G accounts in government and industry reports, highlighting expectations of equipment manufacturers, mobile service operators, and state actors. Our review of documentation illustrated the predominance of a positive view of 5G outcomes in respect to the interests of these actors in

the growth of the economy and industry competitiveness, as well as in protecting the rights of citizens. Principally, 5G is treated as a strategic investment for stimulating economic growth by building momentum in mobile equipment markets and in multiple mobile service using sectors (Organisation for Economic Co-operation and Development [OECD], 2020). The International Telecommunication Union's (ITU) 5G "vision," for example, positions this network architecture as bringing "new unique network and service capabilities" and generating substantial global revenues (International Telecommunication Union—Radiocommunication Sector [ITU-R], 2015, p. 6). The World Economic Forum (WEF, 2020) claims that enhanced connectivity, supported in part by 5G, will boost the IoT market and that multiple industry sectors will benefit from 5G's enhanced AI-enabled functionality enabling enhanced data collection and processing on the peripheries of communication networks.

Most government and industry reports highlight the benefits of a 5G network designed to intensify the use of algorithms and machine learning. They acknowledge potential risks and harms associated with 5G's vulnerabilities to security threats, but, typically, these are said to need to be addressed without slowing 5G deployment (House of Commons, 2020). It may be recognized that "it is becoming increasingly difficult to safeguard privacy as devices become more pervasive and embedded in people's lives, capturing personal data with greater frequency and granularity" (WEF, 2020, p. 6), but there is little evidence of questioning in policy or "vision" statements of the benefits of 5G technical innovation. Consistent with the dominant digital innovation social imaginary, it is expected that data-driven economic growth, stimulated by investment in 5G networks, can be coupled with technical standards that design in features aimed at minimizing 5G risks to citizens' fundamental rights. Thus, 5G is promoted as the "realization of a datafied dreamworld" (Mattern, 2019, para. 8), one that can unleash innovation and enable new profitable data markets to emerge.

Typically, security issues are depicted as an external threat originating in foreign countries, predominantly China. Corporate and state actors are positioned in a global leadership race to achieve success in a data economy inflected by geopolitics—the West being in an "arms race" with the "East." For example,

> if the United States and Europe work together, . . . governments and businesses alike will be in a much stronger position to properly manage the PRC [People's Republic of China] as a systemic rival and shape the future of technological development. . . . (U.S. Congress, 2020, p. 61)

Multiple reports echo a fear that Huawei and other Chinese 5G-equipment vendors will permit the Chinese State to access sensitive security intelligence and to collect and process users' personal and transaction data. When rollouts of 5G networks started in 2019 with 5G trials and marketing of 5G-ready handsets, Western national (and regional) policy makers began to make claims about the insecurity of Chinese mobile network technologies. Western states were depicted as positioning themselves to counter perceived imminent threats to security and to strengthen the position of their equipment manufacturers in the global market.

These expectations about 5G are visible across the three areas (the United States, the European Union, and the United Kingdom) we included in our research. In the United States, for instance, a president's

executive order prohibited online transactions using technology or services "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" (U.S. Executive Office, 2019, p. 22690). This order effectively halted procurement of Chinese telecommunication equipment. Then U.S. Secretary of State, Mike Pompeo, commented in 2020 that "we will keep doing all we can to keep our critical data and our networks safe from the Chinese Communist Party" (Hartman, 2020, n.p.). Specifically targeting next-generation mobile networks, the Secure 5G and Beyond Act (U.S. Congress, 2020) called for a plan to reduce vulnerabilities linked to wireless communication equipment, and this was echoed in a report of the U.S. Senate (United States Senate Committee on Foreign Relations, 2020). The U.S. policy position is justified as a way of "connecting cybersecurity with profitability" (Solarium Commission, 2020, p. 74). It aims to avoid a situation in which "authoritarian states will take advantage of preferred relationships with technology firms to build backdoors for government access that allow them to monitor the private lives of citizens and political opponents at home and abroad" (Solarium Commission, 2020, p. 17).

5G rollout plans in the United Kingdom were linked to a prospective free trade deal and to the stability of security intelligence sharing arrangements with the United States. Then U.S. National Security Adviser, Robert O'Brien, said that, "they [Huawei] are just going to steal wholesale state secrets, whether they are the UK's nuclear secrets or secrets from MI6 or MI5" (Buncomb, 2019, n.p.). After partial measures were taken to reduce British mobile operator dependence on Huawei equipment, the British government instructed these operators to remove Huawei equipment from their 5G and earlier generation mobile networks.

The European Commission has encouraged investment in 5G with an action plan emphasizing the need for technical standards to ensure global network interoperability (European Commission, 2016), but, at the same time, its Cybersecurity Strategy for the Digital Decade signals external cyber vulnerabilities and aims to reduce "dependence on other parts of the globe for the most crucial technologies" (European Commission, 2020, p. 11). The security threat is attributed to China's role in 5G international standardization, which "is increasingly used by third countries to advance their political and ideological agenda, which often does not correspond with the values of the EU" (European Commission, 2020, p. 27). The regional security, competitiveness, and profitability of European companies in the data economy are linked through the aim to integrate 5G and AI in "secure-by-design services" (European Commission, 2020, p. 8).

In each of these contexts, the imaginary is predominately one of an unethical Chinese State (alongside Russia, Iran, and North Korea), and its companies, which are deemed to be influenced by state control over their technology development. The justification for according "bad" actor status to Chinese companies such as Huawei is that the Chinese State requires "any data collected on any Chinese-made product or service to be confiscated by the Chinese government for any reason" (Layton, 2020, p. 2). China's Cybersecurity Security Law asserts state sovereignty over products and services made in China, and its National Intelligence Law requires Chinese subjects to transfer data to the State on request (Creemers, Triolo, & Webster, 2018). This view is contrasted with "good" actors in the United States and other Western countries when it is assumed that, notwithstanding differences in their security and data protection regulations as applied to 5G (Federal Communications Commission [FCC], 2019; United Kingdom

Government, 2022), they will materialize security and privacy standards consistent with the protection of privacy and other public values.

In summary, our review of 5G documentation affirmed that considerable prominence is given to data monetization and the expansion of the data economy. Additionally, the 5G standards implemented by Western-owned companies are either assumed to be implemented to protect citizens' rights when data processing and automated decisions are supported by 5G networks, or it is assumed that they will be soon. Any sources of harms or threats associated with 5G are externalized to China or other non-Western states.

5G Reporting in the United Kingdom Press

Our content analysis of 5G coverage in a sample of British newspapers (N = 795 articles) revealed reporting of a relatively narrow set of 5G benefits, risks, and controversies, and was consistent with our review of documentation in the preceding section.[3] Press coverage emphasized the innovative features of 5G applications and, of 227 descriptive mentions of 5G, 50% referred to 5G as a risk, 21% as a threat, with 9% describing it as revolutionary; and there were 114 mentions of a competitive race. The relation between 5G and data or AI was mostly discussed as a security issue related to foreign interference. In 244 (31% of 795) articles, 25% were about security, 21% about foreign government data access, or foreign company data access (14%). State access to data and other illegitimate actors' access to data (e.g., black hat hackers, terrorists, perpetrators of cybercrime, or terrorists) received exceedingly little attention.

Our content analysis illustrated the predominance of coverage that externalizes 5G risk with a focus particularly on the Chinese company, Huawei. Some 63% or 498 (of 795) articles referred to Huawei's participation in the British 5G network.[4] When a view was reported, it was predominantly negative (47%) or neutral (48%), and there was no significant relationship between the likelihood of mentioning Huawei and a competitive race between companies or countries.[5] However, Huawei was linked to then President Trump's or the U.S. policy position 424 times (53%). When this link was made, it was mainly in reference to security (28%) or trade (16%), with trust or privacy barely mentioned. When reporting of Huawei

[3] The sample was collected for January 1, 2017–March 7, 2020. After cleaning using keywords "5G" and "London" using a Nexis/Lexis search of broadsheets (*The Daily Telegraph*, *The Financial Times*, *The Guardian*, *The Independent* and *The Times*) and tabloids (*Daily Mail*, *Express*, *Daily Mirror*, and *The Sun*), news articles—76% of 795 articles; OpEds 13%, letters to editor, other or unclear 11%. An intercoder reliability check was calculated for each of 157 codebook items, revised for those below IRC = 78% with Yes/No answers and multiple option items. Basic frequency counts and chi-square statistics were used. In this study, we focus on reporting of geopolitical aspects of 5G and note that on these items, there were no significant differences in reporting of 5G benefits and risks by broadsheets and tabloids.

[4] We did not code for other companies, but secondary analysis indicated mentions of the following European companies as candidates to supply equipment for the 5G infrastructure: Ericsson (52), Nokia (56), and Alcatel (4). American-owned companies reported as having a stake in a 5G network were Cisco (7), Qualcomm (19), Altiostar (1), Airspan (1), Mavenir (1), Parallel Wireless (1), Samsung (51) and ZTE (18) mentions.

[5] Huawei mentioned/Tech Race-Competition $\chi^2 = .748$, $p > .05$, not significant.

occurred in relation to the United Kingdom's policy stance toward the company (495 mentions), this relationship was reported as being unclear (57%), but 27% indicated that the United Kingdom should adopt the American policy position on excluding Huawei from participation in 5G construction, with 16% indicating American policy should be resisted. Overall, 5G threats to national security from Huawei were prominent in press reporting and consistent with a social imaginary of digital innovation that externalizes threats. There was very little coverage of the extent to which the materialization of the 5G network would be accompanied by national (regional) or globally transparent responses to privacy or surveillance concerns, with the emphasis instead on the groundbreaking 5G network architecture and its applications.

The foregoing—based on our document review and content analysis of the press—provides little insight into contestations within the dominant social imaginary of digital innovation in the case of 5G's materialization. Neither does it help to assess the extent to which standardization activities are likely to enable features to be designed into standards in a way that gives a priority to the public values expectations embraced by alternative digital innovation social imaginaries. Thus, our case study of OpenRAN below highlights how contradictory values operate within a broader social imaginary by focusing in greater depth on choices about the selection of network architecture and technical standards.

OpenRAN Standardization

Technical standardization is a stage upon which values embraced by a social imaginary become embedded in technology designs. They condition whether hardware and software designs are transparent and subject to audit by those charged with holding companies to public account. The RAN component of a mobile network is located between the center or core of the network and users' equipment (such as a mobile phone or IoT device). A RAN typically consists of a radio unit (the antenna visible on top of a tower) and a baseband unit (devices linking the radio equipment to the core network). The decentralized and virtualized architecture of 5G networks creates opportunities to destabilize the conventional equipment procurement practices of mobile service providers. Our analysis of tensions in this area provides insight into contests over 5G's materialization within the dominant social imaginary of digital innovation and the extent to which features of an alternative imaginary is in play.

A core issue of 5G RAN component standardization is whether it favors a multivendor equipment environment in which equipment supplied by different vendors is mutually compatible (or interoperable). This would represent a significant change insofar as mobile communication operators tend to procure their 5G equipment from a few suppliers, including Huawei and European companies Nokia and Ericsson, which had established leading positions in the 5G market by 2019. Standard-setting activity for this mobile equipment is conducted by working groups of international standardization organizations that openly publish standards and operate by consensus. The ITU plays a major role in 5G standards work, as does the European Telecommunication Standards Institute (ETSI) with its Technical Committee on Cybersecurity standards. The 3GPP (3rd Generation Partnership Project), housed within ETSI with international participation, issued a full release of standards for a generic virtualized 5G network in 2020. Network virtualization and greater reliance on AI-enabled software than earlier generation network infrastructures means that the interfaces between 5G equipment components can be opened to enable companies that have yet to establish a leading position in the equipment vendor market to build upon them.

An "OpenRAN" architecture is being developed in this context that can enable mobile operators to procure equipment components from new entrants to the market, meshing them together using standardized interfaces (Brown, 2020), and building on internationally agreed standards for the RAN (3GPP Release-15), which provided for a "split radio" model enabling the unbundling of RAN components. Those favoring the OpenRAN approach focus on creating more intelligent (AI-enabled), open, virtualized, and fully interoperable mobile networks (Nokia, 2021), claiming benefits of improved network agility and flexibility and a stimulus to innovation in the data economy. This procurement strategy is a departure from the bundled equipment procurement approach where all or most of the mobile network equipment is designed and implemented by a leading contractor. In contrast to OpenRAN proponents, defenders of a bundled approach suggest that procurement from multiple vendors is likely to lead to increased costs of coordination because of the need to manage multiple component interfaces and, crucially, that it introduces new security risks because equipment is being procured from multiple suppliers instead of the market leaders. Mobile communication operators mostly have procured their bundled RAN hardware and software from Huawei, Ericsson, or Nokia based on internationally agreed standards.

While RAN procurement might appear initially to be an economic and technical issue, it has geopolitical implications. Tensions within the dominant social imaginary of digital innovation are inspired by national or regional geopolitical and economic interests and, at the time of writing in early 2022, these were beginning to yield a splintering of 5G standards as a result of the development and adoption of standards developed by national or regional coalitions. The shift to modular software running on general purpose hardware is presented by proponents of a multivendor market as creating conditions for fostering innovation and a competitive global 5G equipment market, thus enabling the West to win the race against Chinese market dominance. The claim is that a virtualized 5G network relying on AI-enabled software to manage the network—as is the case with OpenRAN—can open the market to companies specialized in these areas—a market in which American-owned companies are expected to excel (Plantin, 2021).

An examination of which companies are contributing to the specification of the OpenRAN suggests that a clear separation between Western and Chinese approaches is unlikely to occur. Chinese companies are already substantially involved in the design of OpenRAN specifications through their participation in international standardization bodies. For example, the 5G 3GPP had 136 Chinese company participants (and 2 from Hong Kong) with over 712 individual members in 2021 (3rd Generation Partnership Project, n.d.). Standards contributions are often led by Ericsson, Huawei, Nokia, and Chinese representatives (Rutkowski, 2020), and during the Trump Administration, participation by U.S. government representatives—including the Federal Communication Commission (FCC), which is charged with developing security standards for 5G—was relatively low. In addition, the translation of internationally agreed standards into operational design specifications—which is crucial in materializing security safeguards in the construction of OpenRAN technologies—is undertaken by partnership consortia of mobile operators, equipment manufacturers, and government representatives, some including and others excluding Chinese companies. The O-RAN Alliance, for example, has defined numerous open interfaces to support modularity, and it includes American and European equipment vendors alongside Chinese mobile operators and the China Academy of Information and Communications Technology, which by 2021, had the second largest number of participants (Ahmad et al., 2017).

This might suggest that the values and goals of corporate and state actors are reasonably well aligned given their common participation in international standardization. At the same time, however, the United States and its allied countries have been spearheading an OpenRAN Policy Coalition that includes American-owned companies Nokia and Deutsche Telekom, with members from Japan, South Korea, and Spain, but not Chinese-owned companies. Interpreted as a move by the U.S. government to "shut [. . .] out the Chinese" (Morris, 2020, para. 3), it has also been described as a bid by American mobile-service providers and equipment vendors to introduce "non-standard" 5G specifications that are "vague and technically unimplementable" (Forge, Horvitz, Blackman, & Bohlin, 2019).

In summary, inspired by a digital innovation social imaginary that positions Chinese companies as threatening Western security, but aiming to promote standardization that enables companies to establish a leading position in the AI-enabled software components of the 5G market, national, or regional (American-led or European) standards are depicted as offering more robust data security and privacy protections compared to the protections offered by internationally agreed standards. Thus, standardization initiatives around the OpenRAN are splintering 5G deployments. It is claimed, nevertheless, that Western 5G implementations will protect users from harmful surveillance and privacy intrusions emanating from the "bad" Chinese actors.

This examination of the values informing 5G OpenRAN standards activity illustrates some of the contradictions within the dominant social imaginary of digital innovation. Although choices are depicted as being in line with a defense against external China security threats, it illustrates the instability of the dominant social imaginary in view of the largely U.S.-led aspiration to attain a commanding lead in the global 5G market. In the wider context of geopolitical tensions among the United States, European (and United Kingdom), and Chinese actors, a splintering of the 5G standardization process is unsurprising given the emphasis in the dominant social imaginary on expectations about who can win the 5G equipment and data marketization race. The result is that although claims are made about "local" standards effectively addressing data security breaches and privacy concerns, little attention is given to which actors are most likely to materialize these claims and how they might be held to account if they fail to do so.

Reading 5G Expectations Differently

Our account of 5G's materialization thus far indicates how 5G is suggestive of the dominant social imaginary of digital innovation, including the tensions and contradictions of this imaginary. In this section, we consider our evidence differently, calling attention to potentials for the emergence of an alternative social imaginary of digital innovation that might begin to shape 5G infrastructure development. Such an imaginary would privilege public values and heighten awareness of how the virtualized 5G network architecture itself enhances the risks of intrusive surveillance. This matters because it is theoretically possible for any 5G vendor to gain "clandestine" remote access to data and "the U.S. itself is a well-known practitioner of that capability" (Rutkowski, personal communication, February 24, 2020). In this view, *any* 5G implementation should be treated as creating a heightened risk of privacy intrusions and surveillance, regardless of country of origin of the equipment manufacturer.

Critical scholarship acknowledges that it is not only the Chinese State or China-based companies (or other non-Western actors) that are involved in digital innovation with the potential to jeopardize citizens' fundamental rights. In the United Kingdom, for example, the Investigatory Powers Act has not prevented the home office and the National Crime Agency from gathering data and metadata from Internet service providers about citizen website visits without public transparency (Burgess, 2021). Claims by Western countries about a high risk of state-led surveillance because of the insecurity of Chinese 5G technology compared to technologies developed using splintered Western standards need to be weighed against the American Department of Defense's (DoD, 2020) ambitions to influence 5G standards. At least potentially, these standards heighten the risk of privacy intrusions and surveillance because they involve a splintering of standards that have not met with international approval.

Thus, while Western claims about Huawei and other Chinese 5G manufacturer threats to national security are consistent with the dominant digital innovation social imaginary, they are contradictory insofar as they conceal the commercial goals of states or regions that are vying to establish their own companies' global market leadership. This is illustrated by the U.S. promotion of "home-grown" 5G technologies and "local" standards. Western states and their companies also claim that Chinese State interventions distort competition in the global market by providing R&D and other subsidies, yet the U.S. government provides incentives for 5G investment by its domestic companies (FCC, 2016) and the United Kingdom (House of Commons, 2021) and the European Union (European Commission, 2016) are also providing government support for 5G investors.

In debates about 5G, there is occasional discussion about the need for a Western response to human rights abuses in China, and this may be used to justify banning Chinese equipment vendor participation in 5G network build-outs (Solarium Commission, 2020; Wintour, 2020). However, this concern with human rights and the safety and security of people within China does not appear as a principal motivation for the largely American-led campaign to ensure that Chinese companies do not succeed in expanding their role in building out global 5G networks. Instead, accusations against China as a threat to Western national security can be interpreted as a strategy to suppress efforts to call attention to Western countries' engagement in similar privacy intrusions and surveillance practices. An alternative social imaginary of digital innovation that acknowledges the potential of the enhanced virtualization of 5G networks to extend the datafication capacities of any state, not only China, is thereby largely rendered invisible. As a Dutch report emphasizes, it is important to focus on all digital technologies, not simply those developed by Huawei and other Chinese companies or on 5G alone. All of these infrastructural technologies involve vulnerabilities—"100% security does not exist" (Rathenau Instituut, 2021, p. 4).

The values linked to an alternative social imaginary of digital innovation occasionally do surface. Discussions about public values and the need for citizen protections and safeguards are often present in 5G (and RAN) standards documentation. But with the splintering of standards that depart from universally agreed technical designs and network architectures for privacy and data protection, the chances of ensuring that robust protections are built into the 5G infrastructure "root" are diminished. Through the participation of multiple actors in the international standardization process, there is at least the potential for recognition of values embraced by an alternative digital innovation social imaginary. Nevertheless, the claims persist that "local" standards and their implementation in 5G equipment designed by Western vendors will be

subject to independent testing and certification that will protect Western countries' citizens from security threats, *whatever their origin*.

Western national or regional ambitions for leadership in the 5G market cannot be taken for granted, however. There may be opportunities to materialize the 5G infrastructure in a way that is better aligned with an alternative social imaginary. For example, mobile communication operators and equipment vendor costs may increase because of the challenges of integrating modular hardware and software components built around "local" standards for the OpenRAN. Mobile service operators may be averse to the risks of dealing with new equipment vendors without a trusted track record. Nokia and Ericsson could maintain a commanding market lead and they continue to participate in and influence international standardization activities. In addition, the risks associated with data insecurity and privacy breaches in the data economy are becoming subject to heightened public debate (Moore & Tambini, 2022), especially in relation to the "trunk" and "branch" components of the digital infrastructure. This may result in more robust policy debate about whether to encourage investment in 5G networks before assurances of privacy protection and data security. The WEF (2020) notes, for instance, that "it is becoming increasingly difficult to safeguard privacy as devices become more pervasive and embedded in people's lives, capturing personal data with greater frequency and granularity" (p. 6). It even suggests considering banning some IoT applications that rely on the "root" of the communication infrastructure, a position inconsistent with values embraced by the dominant digital innovation social imaginary (Mansell & Steinmueller, 2022; Sargsyan, 2016).

The dominant imaginary of digital innovation within which 5G is developing, in summary, might therefore become increasingly unstable if criticism in the West (and potentially in China) of commercial datafication and citizen state surveillance gathers momentum and when challenges are encountered in replacing Huawei equipment (Cerulus, 2021). When concerns are reflected in the press, policy and corporate reports, and in standards outcomes, public values legitimized by an alternative social imaginary of digital innovation could start to influence 5G's materialization more prominently.

Conclusion

Our aim in this study was to apply the social imaginary concept to reveal expectations and choices at the "root" level of the communication infrastructure. We have examined 5G expectations and their materialization in relation to their alignment with a dominant social imaginary of digital innovation and an alternative imaginary favoring public values. Our analysis confirms the overarching expectation that 5G will promote innovative data economy services through the incorporation of AI and machine learning in the 5G network. In the West, beyond the expectation that 5G's virtualized architecture will be superior in opening up opportunities for revenue generating services, our analysis of features of OpenRAN standardization and equipment procurement strategies indicates how little consensus there is about the best way to address an externalized threat to data security that is positioned conveniently as originating with China or other non-Western "bad" actors. We have suggested that 5G materialization simultaneously intensifies commercial datafication and the potential for state surveillance within Western countries with the consequences for human rights protection in the West differing mainly in degree, but not in principle, from those in China (Werbach, 2022).

Our analysis highlights the potential instability of social imaginaries of digital innovation, exemplified by 5G, recognizing that any social imaginary is contested when value contradictions create tensions that shape decisions around the materialization of a new technology. The prevailing dominant social imaginary of digital innovation is associated with expectations that public values (about privacy and data security) will be balanced through international standardization activity with commercial datafication aspirations. Yet the adoption of standards diverging from those agreed internationally to exclude Chinese participation is occurring in response to the goal of attaining success in a competitive market race. The splintering of standardization efforts in support of 5G, and specifically the OpenRAN, appears to be creating a basis for intensifying commercial datafication across economies, and eventually increasing network vulnerabilities.

We also confirm that the materialization of 5G is unfolding as a component of a geopolitical "territorialization project" (Möllers, 2021), the aim being to enable states and countries/regions to manipulate data to secure market dominance. Contradictory values, expectations, and ambitions within the dominant social imaginary are influenced by efforts to exert national or regional control over an AI-enabled, software-dependent, and virtualized 5G architecture, creating risks for states, companies, and citizens. Without a shift toward privileging public values, including the value of democratic and transparent internationally agreed standardization—that is, toward an alternative social imaginary of digital innovation—opportunities to mitigate harms associated with 5G networks are diminished. Our analysis indicates why it is not possible to resolve contradictory values to secure the interests of all 5G actors. It does so by exposing how the dominant digital innovation social imaginary operates to promote the superiority of a new 5G virtualized architecture. At the same time, this imaginary minimizes concerns about 5G's potentially harmful impacts on citizens' fundamental rights to privacy, protections against surveillance, and the threat of reduced decision-making autonomy because of expanding uses of AI, machine learning, and commercial datafication.

A software-dependent, virtual 5G infrastructure is being bound into citizens' lives, and this impacts their capacities to act autonomously. Our analysis reveals what is suppressed or invisibilized by the dominant digital innovation social imaginary. It also emphasizes the importance of an alternative imaginary that may have the potential to heighten expectations for processes of standardization that operate transparently at the international level, yielding greater opportunities for public accountability than does the splintering of standards activity. As public debate gives increasing attention to risks associated with data insecurity and privacy breaches, at least in the Western democracies, there may be new opportunities for the values associated with an alternative digital innovation social imaginary to inflect the deployment of the 5G infrastructure. Our examination of developments at the "root" of the communication infrastructure (Plantin et al., 2018; Van Dijck, 2020) shows why scrutiny of choices at this level is an essential complement to research on infrastructure developments at the "trunk" or "branch" levels. If states and companies are to be held to public account for their actions in an era of ever-expanding commercial datafication, ongoing investigations on all three levels are needed.

Our analysis of imaginaries influencing 5G's implementation is limited insofar as we have not traced how contradictory values are shifting through time. Our multimethod approach also does not permit a fine-grained examination of the participation of individual actors within each state and company in the

stabilization or destabilization of complex imaginaries that shape 5G materializations. However, our analysis has revealed features of the choices and strategies at the "root" level of the communication infrastructure by focusing on developments at the meso-level where institutions—states, companies, and standards organizations—interact with consequences that shape 5G and the broader data economy. Future research is needed to examine how actors perform over time and to detect shifts in priorities to highlight potential opportunities for a reordering of values, thereby giving higher prominence to those associated with an alternative digital innovation social imaginary with stronger emphasis on public accountability and the protection of citizens' fundamental rights.

References

3rd Generation Partnership Project. (n.d.). 3GPP membership page. Retrieved from https://webapp.etsi.org/3gppmembership/QueryForm.asp

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions. *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, 193–199. doi:10.1109/CSCN.2017.8088621

Brayne, S., & Christin, A. (2020). Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social Problems, 68*(3), 628–624. doi:10.1093/socpro/spaa004

Brown, G. (2020). *TIP OpenRAN: Toward disaggregated mobile networking, heavy reading white paper*. Telecom INFRA Project. Retrieved from https://telecominfraproject.com/tip-openran-toward-disaggregated-mobile-networking/

Buncomb, A. (2019, December 24). U.S. national security adviser warns U.K. that China's Huawei will "steal state secrets." *The Independent*. Retrieved from https://www.independent.co.uk/news/world/americas/huawei-us-national-security-uk-china-theft-warning-a9259596.html

Burgess, M. (2021, March 11). The U.K. is secretly testing a controversial web snooping tool. *Wired UK*. Retrieved from https://www.wired.co.uk/article/internet-connection-records-ip-act

Calhoun, C. (2002). Imagining solidarity: Cosmopolitanism, constitutional patriotism, and the public sphere. *Public Culture*, *14*(1), 147–171. doi:10.1215/08992363-14-1-147

Cerulus, L. (2021, November 30). *Cracks appear in West's 5G strategy after Huawei*. POLITICO. Retrieved from https://www.politico.eu/article/us-europe-5g-strategy-huawei/

Creemers, R., Triolo P., & Webster, G. (2018, June 29). *Translation: Cybersecurity Law of the People's Republic of China (effective June 1, 2017)*. Retrieved from http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for Capitalism*. Stanford, CA: Stanford University Press.

Crawford, K. (2021). *The atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. New Haven, CT: Yale University Press.

Department of Defense. (2020, December 15). *Department of Defense 5G strategy implementation plan: Advancing 5G technology & applications securing 5G capabilities*. U.S. Department of Defense. Retrieved from https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf

European Commission. (2016). *Communication—5G for Europe: An action plan and accompanying staff working document*. Shaping Europe's Digital Future—European Commission. Retrieved from https://ec.europa.eu/digital-single-market/en/news/communication-5g-europe-action-plan-and-accompanying-staff-working-document

European Commission. (2020). *The EU's cybersecurity strategy for the digital decade (JOIN(2020) 18 final)*. Joint Communication to the European Parliament and the Council. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York, NY: St. Martin's Press.

Federal Communications Commission. (2016, September 15). *America's 5G future*. Federal Communications Commission. Retrieved from https://www.fcc.gov/5G

Federal Communications Commission. (2019). *Protecting against national security threats to the communications supply chain through FCC programs*. Federal Communications Commission FCC 19-121. Retrieved from https://www.fcc.gov/supplychain

Forge, S., Horvitz, R., Blackman, C., & Bohlin, E. (2019). *Light deployment regime for Small-Area Wireless Access Points (SAWAPs): Final report*. SCF Associated Ltd. Retrieved from http://op.europa.eu/en/publication-detail/-/publication/463e2d3d-1d8f-11ea-95ab-01aa75ed71a1/language-en/format-PDF

Gillespie, T. (2017). Governance of and by platforms. In J. Burgess, T. Poell, & A. Marwick (Eds.), *The SAGE handbook of social media* (pp. 254–278). London, UK: SAGE Publications.

Hartman, L. (2020, December 17). *Expanded clean network initiative safeguards data*. U.S. Embassy in Georgia. Retrieved from http://ge.usembassy.gov/expanded-clean-network-initiative-safeguards-data/

House of Commons. (2020). *Security of 5G, second report of session 2019–21*. House of Commons Defence Committee, HC201. Retrieved from https://committees.parliament.uk/publications/2877/documents/27899/default/

House of Commons. (2021). *5G market diversification and wider lessons for critical and emerging technologies, second report of session 2019–21*. House of Commons Science and Technology Committee. Retrieved from https://committees.parliament.uk/publications/4551/documents/46156/default/

International Telecommunication Union—Radiocommunication Sector. (2015). *IMT vision—Framework and overall objectives of the future development of IMT for 2020 and beyond—Recommendation ITU-R M.2083 (09/2015)*. International Telecommunication Union.

Layton, R. (2020). *The security of 5G: Written evidence submitted by Roslyn Layton*. Ministry of Defence, Second Report of Session 2019-21, HC 201, SFG0017. Retrieved from https://committees.parliament.uk/writtenevidence/1837/default/

Mansell, R. (2012). *Imagining the internet: Communication, innovation and governance.* Oxford, UK: Oxford University Press.

Mansell, R., & Plantin, J.-C. (2020). *Urban futures with 5G: British press reporting (Media@LSE Report)*. Department of Media and Communications, London School of Economics and Political Science. LSE Research Online. Retrieved from http://eprints.lse.ac.uk/105801/

Mansell, R., & Steinmueller, W. E. (2020). *Advanced introduction to platform economics*. Cheltenham, UK: Edward Elgar Publishing.

Mansell, R., & Steinmueller, W. E. (2022). Denaturalizing digital platforms: Is mass individualization here to stay? *International Journal of Communication, 16*, 461–481. Retrieved from https://ijoc.org/index.php/ijoc

Mattern, S. (2019, July 8). *Networked dream worlds: Is 5G solving real, pressing problems or merely creating new ones?* Retrieved from https://reallifemag.com/networked-dream-worlds/

Meng, B. (2021). "This is China's Sputnik moment": The politics and poetics of artificial intelligence. *Interventions*, *0*(0), 1–19. doi:10.1080/1369801X.2021.2003227

Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology, & Human Values, 46*(1), 112–138. doi:10.1177/0162243920904436

Moore, M., & Tambini, D. (Eds.). (2022). *Regulating big tech: Policy responses to digital dominance*. Oxford, UK: Oxford University Press.

Morris, I. (2020, June 5). The political hijacking of open RAN. *Light Reading*. Retrieved from https://www.lightreading.com/5g/the-political-hijacking-of-open-ran/a/d-id/759454

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: NYU Press.

Nokia. (2021). *Open RAN*. Nokia. Retrieved from https://www.nokia.com/networks/portfolio/radio-access-networks-ran/open-ran/

Organisation for Economic Co-operation and Development. (2020). *OECD digital economy outlook 2020*. Organisation for Economic Co-operation and Development. Retrieved from https://www.oecd-ilibrary.org/sites/bb167041-en/index.html?itemId=/content/publication/bb167041-en

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Plantin, J.-C. (2021). The political hijacking of open networking. The case of open radio access network. *European Journal of Communication, 36*(4), 404–417. doi:10.1177/02673231211028375

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society, 20*(1), 293–310. doi:10.1177/1461444816661553

Powell, A. B. (2021). Explanations as governance? Investigating practices of explanation in algorithmic system design. *European Journal of Communication*, *36*(4), 362–375. doi:10.1177/02673231211028376

Rathenau Instituut. (2021, March 11). *Dutch debate on 5G needs more substance*. Rathenau Instituut. Retrieved from https://www.rathenau.nl/en/message-to-parliament/dutch-debate-5g-needs-more-substance

Rutkowski, A. (2020, December 14). *Remediating U.S. 5G global supply chain security engagement*. Retrieved from http://www.circleid.com/posts/20201214-remediating-us-5g-global-supply-chain-security-engagement/

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication, 10*, 2221–2237.

Solarium Commission. (2020). *Cyberspace Solarium Commission report*. Solarium Commission. Retrieved from https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view?usp=embed_facebook

Taylor, C. (2002). Modern social imaginaries. *Public Culture*, *14*(1), 91–124. doi:10.1215/08992363-14-1-91

Taylor, C. (2007). *A secular age* (1st ed.). Cambridge, MA: Harvard University Press.

Turow, J. (2017). *The aisles have eyes: How retailers track your shopping, strip your privacy, and define your power*. New Haven, CT: Yale University Press.

United Kingdom Government. (2022). *The electronic communications (security measures) regulations.* Statutory Instruments No. 933. Retrieved from https://www.legislation.gov.uk/uksi/2022/933/contents/made

U.S. Congress. (2020). *Secure 5G and Beyond Act of 2020 (2019/2020), Public Law No. 116-129*. United States Publishing Office. Retrieved from https://www.congress.gov/bill/116th-congress/senate-bill/893/text

U.S. Executive Office. (2019). Securing the information and communications technology and services supply chain, Executive Order 13973. US President Executive Order. *Federal Register, 84*(96), 22689–22692. Retrieved from https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf

United States Senate Committee on Foreign Relations. (2020). *The United States and Europe: A concrete agenda for transatlantic cooperation on China. SFRC majority China-Europe report*. United States Senate Committee on Foreign Relations Majority Report. Retrieved from https://www.foreign.senate.gov/imo/media/doc/SFRC_Majority_China_Europe_Report_FINAL_P_and_G.pdf

Van Dijck, J. (2020). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society, 23*(9), 2810–2819. doi:10.1177/1461444820940293

Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford, UK: Oxford University Press.

World Economic Forum. (2020, December 11). *The State of the connected world: 2020 edition*. World Economic Forum Insight Report with Global IoT Council. Retrieved from https://www.weforum.org/reports/state-of-the-connected-world-2020-edition

Werbach, K. (2022). Orwell that ends well: Social Credit as regulation for the algorithmic age. *University of Illinois Law Review, 2022*, 101–157. doi:10.2139/ssrn.3589804

Wintour, P. (2020, July 14). The Huawei dispute is only one part of a wider UK-China struggle. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2020/jul/14/the-huawei-dispute-is-only-one-part-of-a-wider-uk-china-struggle

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: Public Affairs.