Article

Infrastructural surveillance

new media & society
2020, Vol. 22(8) 1414–1436

DOI: 10.1177/1461444819879426
journals.sagepub.com/home/nms
SAGE

Alex Gekker
University of Amsterdam, The Netherlands

Sam Hind
University of Siegen, Germany

Abstract

This article proposes a new model of privacy: infrastructural surveillance. It departs from Agre's classic distinction between surveillance and capture by examining the sociotechnical claims of connected and autonomous vehicles (CAVs) as requiring totalising surveillance of passengers and environment in order to operate. By doing so, it contributes to the ongoing debate on the commodification and platformisation of life, paying attention to the under-explored infrastructural requirements of certain digital technologies, rather than its business model. The article addresses four distinct characteristics of infrastructural surveillance: the aggregation of data, initialisation of protocols limiting possible actions, the prioritisation of distributed modes of governance and the enclosure of the driver in a personalised bubble of sovereign power. Ultimately, unlike previous modes of computer privacy in which activities are being constructed in real time from a set of institutionally standardised parts specified by a captured ontology, we observe the creation of new ontologies.

Keywords

Connected and autonomous vehicles (CAVs), datafication, driving infrastructure, ontology, platformisation, privacy, protocols, sensors, surveillance and capture

There is a scene in Steven Spielberg's 2002 sci-fi thriller *Minority Report*, in which the protagonist discovers, while driving, that he has been accused of a crime that he did not

Corresponding author:
Alex Gekker, Faculty of Humanities, University of Amsterdam, Turfdraagsterpad 9, BG1, Room 2.19, 1012 XT Amsterdam, The Netherlands.
Email: a.gekker@uva.nl

commit and from which he cannot be acquitted. His car's mechanical voice calmly informs him that his destination has been changed, and that he is no longer in control of the vehicle. Thus, his only option becomes smashing the windshield and escaping the car itself. While various people have *escaped* in films, never in the popular imagination has the car itself, along with the infrastructural network that allows for its existence, been vilified as much as in the scene described above. The personal car, in particular – independent of public transport infrastructure and connected to the (American) imagination of freedom (Cross, 2018; Flink, 1976; Steg, 2005) – is often *a means* through which escape is possible. To be certain, fictional characters have also escaped *from* cars, put there as unwilling prisoners of various antagonists. But even in such a case the car *itself* is an object devoid of malice; even possessing the potential for redemption. To wrestle away the vehicle's control from the villain is to gain newfound agency and become the master of your destiny again (Wollen and Kerr, 2002). However, in a society where the car is *autonomous*, and thus potentially dominating its user, *Minority Report* posits a protocological argument (Galloway, 2004): to be mobile is to be visible, and to be visible is to be controlled.

While far from their fictional depictions, connected and autonomous vehicles (CAVs) are a growing category of automobiles that possess an array of sensors and calculative powers (Alvarez León, 2019b; Bissell, 2018; Hind, 2019) that not only enables, but requires, them to collect large amounts of traceable and ostensibly attributable personal data. While prototypical autonomous vehicles have garnered significant interest in the wider public sphere, concerning their presumed safety (or lack thereof), 'connected' vehicles have received marginal coverage (Marres, 2018 notwithstanding). This is despite a European Union (EU) ruling on the mandatory inclusion of an emergency 'ecall' service in all new vehicle models (European Parliament, 2014), and recent battles over the communicative default – Wi-Fi or cellular – for CAVs across EU member states (Drozdiak, 2019; Drozdiak and Rolander, 2019). Like other developments in the automobile world such as the use of social navigation apps (Hind and Gekker, 2014), we take CAVs to be significant objects of study, shaping mediated lives today.

This article expands on the recent debates on the intermingling of platforms (Barns, 2019; Murakami Wood and Monahan, 2019; Zuboff, 2019), infrastructures (Helles and Flyverbom, 2019; Parks and Starosielski, 2015; Plantin and Punathambekar, 2019) and modes of global governance (Bratton, 2015; Easterling, 2016). Our article takes the CAV as an object through which questions of mobility, surveillance and choice can be asked. Specifically, we interrogate the privacy ramifications of the imbrication of quotidian actions (to drive) and surveillance processes (to be visible), as encapsulated above. We do this by building on previous work arguing that the ontological division between map and territory has collapsed with the advent of CAVs (Hind and Gekker, 2019). Our main claim is that certain modes of technological devices have become predicated on totalising knowledge of their subjects' conditions in order to function. However, unlike the notions of dataveillance (Amoore and De Goede, 2005; Clarke, 1988), platform commodification (Van Dijck et al., 2018) surveillance capitalism (Zuboff, 2015, 2019) or platform surveillance (Murakami Wood and Monahan, 2019) our conceit largely sidesteps the business models, value propositions and marketing techniques of the digital giants involved. Instead, we focus on the proposition offered by a growing number of ‘smart-’ and data-driven technologies in which user surveillance is stated as a necessary precondition for its operation. We use the CAV to offer a larger conceptual framework to interrogate such developments.

Our argument proceeds through three stages. In the first, we review Philip Agre’s (1994) classic work suggesting two types of privacy to establish the groundwork of thinking about surveillance. In the second, we examine how the notion of contemporary media infrastructures complicates some of Agre’s presuppositions. In doing so, we focus attention on data aggregation, standards, the distribution of knowledge production, and the valorisation of knowledge enclosure to challenge the surveillance and capture models of privacy he offers. To rectify, in the third part of the article we posit the hybrid model of *infrastructural surveillance*, which combines some characteristics of the two to create a model of privacy in which ‘opting out’ is problematic. We demonstrate this hybrid model with reference to CAVs, which pose novel privacy issues regarding how data are collected, circulated, utilised and valued.

The capture model and its limitations

In the mid-1990s, the world was waking up to the massive computerisation of work and leisure, asserting new forms of political, economic and cultural relations (Castells, 1996; Meyrowitz, 1985; Negroponte, 1995). Among other aspects, miniaturisation and mobility of electronic equipment allowed for seemingly unprecedented levels of communication. Early in the spread of Wi-Fi and cellular networks, media scholar Mark Poster noted that while information has always been mobile in distinct ways, technology does add something new to the capacities of such mobility. Traditionally, as in the case of the semaphore or the telegraph, sociotechnical systems allowed for information to be moved between static human interlocutors. Second, some forms of communication allowed mobile humans to carry static information with them, for example, as books, letters or music on the Walkman or an iPod. However,

> [m]ore recently mobile communications has taken on a third meaning. Internet technology, wired and wireless, enables individuals to move and at the same time to generate information, transmit information, and receive information designated for them . . . individuals may move through space and the information will accompany them, find them, or even tell them where they are, as in Global Positioning Systems. Communication and people then travel together everywhere. (Poster, 2004: 1–2)

Alongside optimism, the era ushered in new fears of technological domination. As per the quote above, the imbrication of movement with communication in real-time digital scenarios has drastically changed the meaning of being *located*. This historical context helps us to understand the classic work of Philip Agre (1994) on privacy in digitised (then computerised) environments. His main goal was not to discard privacy concerns, but rather to emphasise that the fear of one’s loss of privacy expressed through the then dominant model of *surveillance* was mistaken. To him, this model was rooted in visual metaphors of invasion and malice. Instead, he differentiated a *capture* model of privacy, centred on linguistic metaphors of computers and data-processing: lacking any connotation of doing harm to the 'captured' data from a large corpus of text data collected routinely, unlike when a governmental agent surveys a possible target.

Agre suggests that the capture model is a better contextual way to approach privacy issues today. This model remains central to the work of media scholars today, working on issues of space, labour and power (Galloway, 2006; Kitchin, 2014; Suchman, 1995). Moreover, the capture model's central organisational metaphor remains essential, as it is predicated on understanding 'grammars of action' or the way information is parsed and categorised by computers in complex processes. Specifically, Agre notes that the computerisation of the workplace exacerbates the *sequencing* and *ordering* of work processes, which he traces from the historic application of Taylorism and scientific work management. Labour is broken into the most basic 'minimum replicable units' (Quinn, 1992, as cited in Agre, 1994: 108) to be traced, preserved and compared. The application of measurement to such actions as assembly-line stages or the flow of paperwork within and between departments is then described as 'natural' and existing a-priori (thus committing to the fallacy of computation as neutral political force) before being reinstated in digital code, becoming stratified.

This leads to what Galloway (2004) refers to as protocological power, observing that actors in such a state are bound not necessarily by the content or intention of their actions, but by whether such actions are permissible under the (sociotechnical) transmission protocols of the organisation. Think, for example, of the bureaucracy involved in submitting an expense claim: the form-filling, box-ticking and receipt-filing. Protocological systems exacerbate this by codifying the rules of transmission in software and hardware, removing the possibility for human consideration. We can link it to Bogost's (2006, 2007) identification of procedural rhetoric as the specific persuasive form that digital objects apply on their subjects, where the 'argumentation' occurs on the systemic level of which buttons are 'greyed out' on a computer screen in response to previously checked tick-boxes. Agre similarly recognises the inherent dangers of computerisation as the quiet coercion of its subjects to conform and alter their behaviours to within the expected parameters of the system (cf. Beer, 2015). And so, his two models of privacy – not mutually exclusive, but contingent – are intended as conceptual tools to analyse discursive regimes (Table 1).

Overall, our argument for infrastructural surveillance breaks away from the capture model at the point of translation. Whereas the captured actions (form-filling, box-ticking) are operationalised from existing a-priori multitudes of life, under 'smart' technologies no actions are possible outside of the bounds allowed by the infrastructure. Privacy is thus not threatened after the fact, but is constrained as a matter-of-fact. Participation is dependent on the agreement to be surveilled and immediately curtailed by such surveillance.

The best example of this can be seen in trying to apply the grammars of action logic onto CAVs. Agre (1994) underscores the potential agency of those within the system by highlighting the feedback loop between the physical activity performed and the captured data undertaken:

> [J]ust as the speakers of English can produce a potentially infinite variety of grammatical sentences from the finite means of English vocabulary and grammar, people engaged in

Table 1. Comparison between surveillance and captured privacy models, based on Agre (1994: 122).

Surveillance	Capture
Employs visual metaphors: Big Brother is watching you.	Employs linguistic metaphors by means of various grammars of action.
Emphasises nondisruptive, surreptitious data collection.	Describes the readily apparent instrumentation that entails the reorganisation of existing activities.
Is concerned to mark off a 'private' region by means of territorial metaphors of 'invasion' and the like.	Activities are being constructed in real-time from a set of institutionally standardised parts specified by the captured ontology.
Depicts the monitoring of activity as centrally organised and presumes that the resulting information is centrally stored.	Emphasises the locally organised nature of activities within particular institutional contexts.
Takes as its prototype the malevolent political activities of state organisations.	Takes as its prototype the quasi-philosophical project of ontological reconstruction undertaken by computer professionals in private organisations.

> captured activity can engage in an infinite variety of sequences of action, provided these sequences are composed of the unitary elements and means of combination prescribed by the grammar of action. (p. 117)

To expand, Agre's grammars of actions are dependent on the pre-existence of an established human practice, such as submitting a workplace expense claim, which is then 'imposed on' and actively shaped by the computerised/digitised grammars; separating out the activity into discrete features (again, box-ticking and receipt-filing). In the case of CAVs, we argue that while there is indeed a pre-existing human practice – the physical act of driving a car – no set or series of grammars is imposed on this activity.

Agre's capture model is thus rendered only partially appropriate, as no capture and grammatisation of primary (human) driving actions take place at all. As we show in the next section, operating a CAV with its many sensors and data collection capabilities implicates the user in adhering to non-grammatised standards as a precondition of being allowed to perform any action whatsoever. While (potentially) exacerbated in fully autonomous vehicles, this can be seen in how driving connected vehicles is affected by decisions from third parties such as digital platforms or city officials (Hind and Gekker, 2014; Van der Graaf and Ballon, 2019). Recalling the initial example, it is similar to an expense claim being automatically assessed and approved, without the need for manual submission or assessment from either claimant or administrator. No human labour is required, no human actions are performed and, thus, there is no imposition of 'correct' or 'ideal' expense practices on humans previously involved in this process. In fact, at some point we can imagine an expense claim being processed automatically, with the employee unaware of any penalties imposed upon them.

Agre explicates that ‘no matter how thoroughly the capture process is controlled, it is impossible, *short perhaps of total mechanisation* of a given form of activity, to remove the elements of interpretation, strategy, and institutional dynamics’ (p. 112, our emphasis). Under the dual processes of platformisation and infrastucturalisation, some platforms become the de facto public space for their users, with daily spatial interactions filtered through their automatic processes (Barns, 2019; Batorski and Grzywińska, 2018). CAVs therefore present a step change to Agre’s impossibility: a cybernetic feedback loop where vehicle movement is predicated on the transformation of space into digital infrastructure without which the world is neither knowable, nor driveable (cf. Kitchin and Dodge, 2007; Rankin, 2016; Thrift and French, 2002).

The infrastructural

In their work on the infrastructural disposition for understanding media, Parks and Starosielski (2015) define media infrastructures as follows:

> [S]ituated sociotechnical systems that are designed and configured to support the distribution of audiovisual signal traffic . . . They are highly automated, relying on sensors and remote control, and require human about for their design, installation, maintenance, and operation. (pp. 4–5)

While vehicles do not necessarily register as ‘media’, this is not as straightforward as it seems. Cars have been implicated with media infrastructure in three distinct ways. First – recalling the opening filmy example of this article – modern media has built up automotive imaginations of infrastructure, from the romanticism of the long train journey to the freedom of American highways (Wollen and Kerr, 2002). Second, media production, from news to blockbusters movies, is greatly enabled and shaped by the possibilities of personal mobility. Finally, and most relevant to our point, the introduction of digital media into the driver’s immediate environment has constituted a modification of the human–machine assemblage and shifted the power balance towards the automated (Thrift, 2004). As Alvarez León (2019b) has remarked, ‘cars have become mobile spatial media environments’ (p. 198). When considering what such a shift does in light of the computational industries’ desire to colonise ever growing segments of human conscious and non-conscious psyche (Berry, 2014; Hayles and Sampson, 2018; Sampson, 2017), a particular image of the driver’s body emerges. This is in line with the ‘infrastructural turn’ in media studies where ‘[c]oming to terms with major digital platforms thus involves paying attention to the aesthetic and affective power that digital infrastructures have come to wield in public cultures across the world’ (Plantin and Punathambekar, 2019: 167).

The third ‘epoch-making’ technology, as identified by Baran and Sweezy (1966), after the steam engine and the railroad system; the automobile drastically reshaped space and time in post-war United States and Europe. John Urry (2004) talks of the ‘system’ of automobility, and the ways in which life is ‘locked into’ the automobile lifeworld, in which ‘[t]his mode of mobility’ while being ‘neither socially necessary nor inevitable’ has ‘seemed impossible to break from’ (p. 27). We must therefore understand the deep archaeologies of transport and media infrastructures, if we are to understand this new model of privacy, located in the simultaneously casual capture of human actions and relentless redirection of them onto, and into, the 'driving-machine' (Hind, 2019).

Media infrastructures, we argue, in the broadest sense, entail the creation of new ontologies. Plantin (2018), for instance, identifies an infrastructural shift in cartography, in which Google Maps moved from being a participatory platform to a 'knowledge infrastructure' (p .494). He explains that

> [t]he Google Maps API is used to power so many applications that it constitutes a de facto standard for online maps. It is reliable and mostly invisible, yet a breakdown of Google Maps would disrupt all the services that depend on it – including business, government, work, and everyday commuting. (Plantin, 2018: 494)

Moreover, 'the creation and the circulation of cartographic knowledge are matters of control over who is mapping, who is mapped, and who can access the map' (Plantin, 2018: 495). Application Programming Interfaces (APIs) here constitute a new way to delimit what mapping entails. While digital platforms are often an integral part of new, expansive media operations, they are only access points into, and products of, rather than precursors to, infrastructures. Infrastructures thus govern the capacities of any platform (Plantin et al., 2018).

The shift of Google Maps from participatory platform to cartographic infrastructure has implications for how geographic data are captured, stored, used and valued. Such a practice is not limited to location-based data, however. Similarly, Helles and Flyverbom (2019) exemplify how Netflix uses its tracking of user habits to optimise the distribution of server locations and content transmission, cementing itself as the entertainment infrastructure. While some have suggested there has been a 'pivot' towards platforms in recent years (Barns, 2019: 2), we argue, after Plantin et al. (2018), that unpacking the issue requires a 'bifocal' view, where the infrastructural nature of large-scale platforms is juxtaposed with the growing platformisation of traditional infrastructures. To do so, in the coming section we outline what we see as the four main characteristics of media infrastructures, following Plantin (2018), and tie them to CAVs, in order to reconnect this to Agre's model.

First, media infrastructures *aggregate* multiple data sources. This involves the development of new infrastructural formations capable of capturing data in different modes, with differing regularity, alongside new kinds of data altogether. As Plantin (2018) argues, Google Maps derives its cartographic data from a range of data sources, including governments and international initiatives (satellite data), local business owners (opening hours) and in-house projects such as Google StreetView (static street imagery). These active data collection techniques are also supported by the passive aggregation of use-data derived from smartphones, smart devices, laptops and desktop computers. These data sources, although each valuable on their own, are necessarily aggregated to provide both a more comprehensive understanding of Google Maps use practices across locations, demographics and devices, as well as a more comprehensive arrangement of cartographic services beyond simply 'a map' (McQuire, 2019). Furthermore, this infrastructural pursuit has also involved the capture of entirely new kinds of data, such as elemental and atmospheric data derived from CAVs, as we will discuss in the following section (Durham Peters, 2015; McCormack, 2017; O'Grady, 2018).

Second, they develop *standards*. This involves the creation of new infrastructural rules and regulations in which to streamline data collection, storage and use throughout the system. As Star (1999) suggests, 'infrastructure takes on transparency by plugging into other infrastructures and tools in a standardised fashion', allowing data sources, for example, to be aggregated (pp. 381–382). Similarly, in Galloway's (2004) discussion of the Internet, he argues it is

> . . . not simply a free-for-all of information 'out there', nor is it a dystopia of databanks owned by corporations. It is a set of technical procedures for defining, managing, modulating, and distributing information throughout a flexible yet robust delivery infrastructure. (p. xv)

Moreover, these protocols are 'material', and network protocols specifically should be considered as 'things that are designed to serve applications, to run on computational platforms, and to control infrastructures, bound up with and contributing to the material realization of them all' (Dourish, 2015: 185). To illustrate, in their recent work on the platformisation of infrastructure (and infrastructuralisation of platforms), Plantin et al. (2018) showcase what happens when a private software entity becomes in charge of prescribing such protocols. They use the example of Facebook's encroachment on the open web – programmable, HTML web pages – and their replacement with proprietary Facebook-compatible ways of accessing and sharing content. They argue that previously open functionality (RSS) is lost in platform-specific functionality (Newsfeeds) that in turn robs those unwilling (or unable) to participate in the platform from the original open affordance. Following Galloway (2004), this renders the question of communicated content secondary to the question of access at all.

The third characteristic of media infrastructures is that they *distribute*, if not decentralise, knowledge production. Here, infrastructure built to aggregate data, according to specific standards, cultivates distributed knowledges in ways that other organisational forms (nation state, Fordist firm) may not. Parks and Starosielski (2015) argue that a 'focus on infrastructure foregrounds *processes of distribution*', in which content delivery practices are foregrounded (p. 5, authors' emphasis). Plantin argues that this constitutes a 'decentralization' (p. 499) in respect to Google Maps, as users contribute to the production of cartographic data by using a variety of Google Maps-based services, albeit while reconstituting a monopolistic centralisation. Similar claims are made with respect to the distributed nature of Facebook as an infrastructural operation, dependent on multiple networks linked via API (Plantin et al., 2018).

Yet the distribution of knowledge production is not the same as decentralisation (cf. Galloway, 2010). Although some media infrastructures distribute knowledge production, they might not necessarily decentralise this process. Arguably, contra to Plantin (2018), Google Maps does not engage in the decentralisation of knowledge production, but merely in its distribution, as McQuire (2019) explores. Here, some sites of knowledge production are prioritised over others (generic app use over desktop edits). In a truly decentralised arrangement, knowledge production at multiple centres would operate with equal value and importance. Nevertheless, the distribution of knowledge production is a notable feature of media infrastructures.

The final characteristic of media infrastructures is the valorisation of knowledge *enclosure* that follows from the distribution we discuss above. Here, the distribution of knowledge production is leveraged, not to create a kind of social commons, but to provide and package viable, and possibly valuable, media assets. APIs, for instance, acting as gateway to restricted functionality aim to '*decentralise* data production while *recentralising* data collection' (Helmond, 2015: 5, our emphasis). We argue that this happens in both direct and indirect ways in relation to CAVs.

Directly, the personal automobile transformed or created entire cottage industries of media to be experienced as 'amalgamation' (Schulz, 2004: 89) of the driving itself, from screens embedded in the back seats of family cars to voice artist recording specialised 'funny' voice packs for GPS (Global Positioning System) navigation (Alvarez León, 2019b). The infrastructure of radio broadcasting in many developed nations is a prominent example with its growing focus on the commuter stuck in traffic, consequently changing scheduling, programming and news focus (Miller, 2015, 2017). CAVs exacerbate such tendencies, making their drivers/riders evermore susceptible to targeted media.

Indirectly, following Nigel Thrift's (2004) argument, the increasing imbrication of driving activities with computerisation – particularly GPS-based – has opened the possibility of reimagining the driver-car as a performative hybrid embedded in the social fabric on the city. We have written elsewhere on further opportunities that social connectivity allows for such hybrids (Hind and Gekker, 2019), but suffice it to say that a case can be made for extending, or overlapping, the notion of 'media infrastructure' onto that of the traditional infrastructures of driving. This is particularly apt as digital giants such as Alphabet (Google), Apple and Uber extend their commercial interest into reshaping urban mobility (Bliss, 2018; Johnson, 2012; Marshall, 2017).

This somewhat challenges Parks and Starosielski's (2015) definition of media infrastructure, particularly in relation to the complex relation of the automobile as a component in the media landscape. Recalling Poster's (2004) third definition of mobile media – information transmitted and received while on the go – the car has profoundly changed the nature of mobile media production and usage. While it is arguable that infrastructures do not enclose knowledge by design, we suggest that CAV infrastructures likely do so in a selective fashion, restricting access to established and accepted infrastructural partners, contractors and operators.[1]

Infrastructural surveillance

Consequently, these infrastructural specificities result in a fundamentally novel form of privacy we call infrastructural surveillance. This is different from platform surveillance (Murakami Wood and Monahan, 2019) or surveillance capitalism (Zuboff, 2015, 2019), because it emphasises the total reformatting of privacy practices along infrastructural lines rather than limiting itself to singular forms (platform surveillance) or macro-economic business logic (surveillance capitalism). In short, infrastructural surveillance gestures towards the largely inescapable nature of sovereign power wielded by some, where platform surveillance does not. In metaphorical terms, infrastructural surveillance is the thread of the ‘technological everyday’ (Barns, 2019: 7), rather than a surface upon which some activities take place.

While particularly visible in the case of CAVs, the framework can be productively extended to multiple emergent technologies, as we discuss towards the end of the article. In this section, we explicate the privacy ramifications of the model by taking the four infrastructural characteristics (after Plantin) detailed in the previous section; in response to the challenges issued to Agre’s capture model. We use the current state of CAVs to examine source aggregation, standard development, the distribution of knowledge production and knowledge enclosure. In other words, we ask, what shape does infrastructural privacy take?

Aggregation

While seemingly compatible with the capture model, infrastructural surveillance does not dedicate itself to the capture and optimisation of a particular activity for its future optimisation. Instead, it aims to acquire and aggregate data that are then analysed in unknown (and potentially unknowable) ways. As Privacy International (2018) suggest, ‘cars have become inaccessible computers which collect increasingly granular data, not just about the car itself, but also behaviours of drivers’ (n.p.). A Telematics Control Unit (TCU) allows data from a variety of sources within a connected vehicle to be collected (Figure 1). The communications network that comprises of a TCU and the many electronic control units (ECUs) throughout a vehicle, is ordinarily referred to as a ‘bus’ (Lawson, 2015: 22). As a Canadian report on CAVs explains,

> Data generated and communicated via the vehicle bus system(s) covers virtually all aspects of vehicle operation including engine temperature, engine RPM, throttle position, vehicle speed and orientation, distance travelled, fuel levels and consumption, door open/close, tire pressure, ignition, headlights/tail-lights, battery status, cumulative idling, odometer, trip distance, braking activity, and much more. With the addition of GPS modules, the vehicle bus data also includes vehicle location information. (Lawson, 2015: 22)

As Privacy International (2018) highlights, this is a privacy issue ‘because for many people driving a car is not a choice’ (n.p.). It necessitates acceptance of data collection that, in various ways, can be used to identify the vehicle and its driver. As law enforcement officers in the United States have suggested, information collected by (future) CAVs about its environment might also be freely accessible, without the need for a warrant. Journalist Cyrus Farivar (2018) has argued in the United States that

> [since] none of us have a ‘reasonable expectation of privacy’ when we are in public . . . just as the police can capture us with video cameras and license plate readers, so, too, could they contract with AV automakers to simply get a vast quantities of future AV data. (paragraph 13)

This is made possible due to the aggregation of data from various components of a CAV, such as notifications of engine temperature, a tracking of braking activity or a recording of trip distance, that signal little by themselves but are worrisome in aggregation.

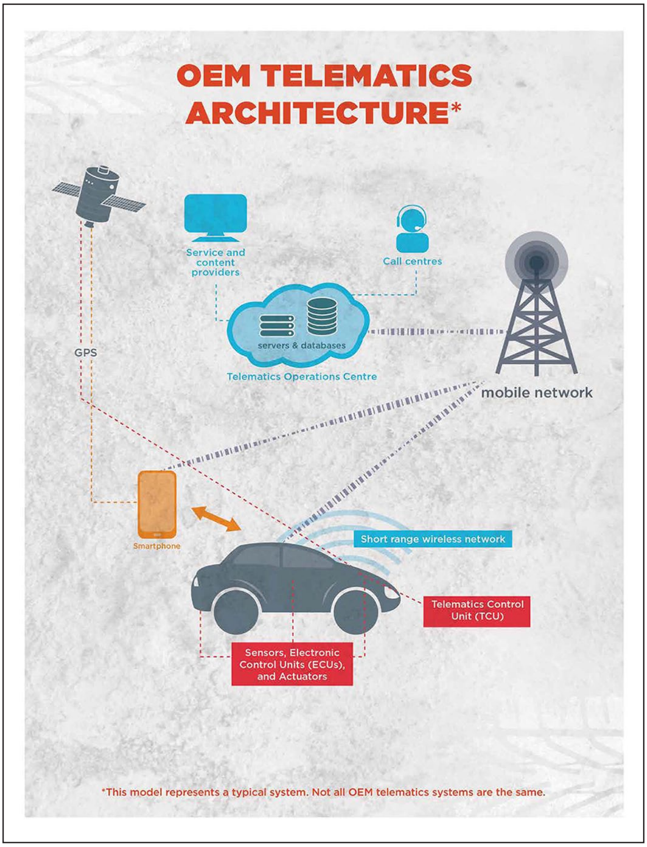

OEM TELEMATICS ARCHITECTURE*
Service and content providers
Call centres
servers & databases
Telematics Operations Centre
GPS
mobile network
Smartphone
Short range wireless network
Telematics Control Unit (TCU)
Sensors, Electronic Control Units (ECUs), and Actuators
*This model represents a typical system. Not all OEM telematics systems are the same.

Figure 1. A typical telematics architecture in a connected vehicle.
Source: Lawson (2015).

Compiled from these different sources, a comprehensive picture of the vehicle can be built: perhaps how the engine suffers from repeated long-distance journeys and consistent hard braking. Consequently, this builds an even more comprehensive picture of the driver and their behaviour. Or at least, this aggregation allows the posing of questions: why the long-distance journeys? Why the hard braking? These are questions that can be asked by a range of parties with accredited access to the aggregated data: vehicle manufacturers, device manufacturers, insurance companies, rental car companies and law enforcement. The telematics architecture of any CAV thus governs the possibility for interrogative extrapolation, predicated on the aggregation of operational data via a vehicle's many ECUs.

In response, Privacy International has suggested that CAVs contravene several 'Data Exploitation Principles'. These include the right to object to personal data contributing to a proprietary or secret intelligence system. They also propose that 'systems should be designed to minimise data generation, processing, and access' and that 'data must be protected from access by persons who are not the user' (Privacy International, 2018: n.p.). In essence, the aggregation of operational data in a CAV actively exploits and exposes drivers in ways markedly different from those witnessed under alternative privacy models. Moreover, the aggregative nature of this operation naturally exceeds any one platform, only made possible by infrastructural arrangements that funnel huge, varied and granular kinds of data through obligatory passage points (Callon, 1986) for opaque, unknown or inaccessible reasons.

Standards

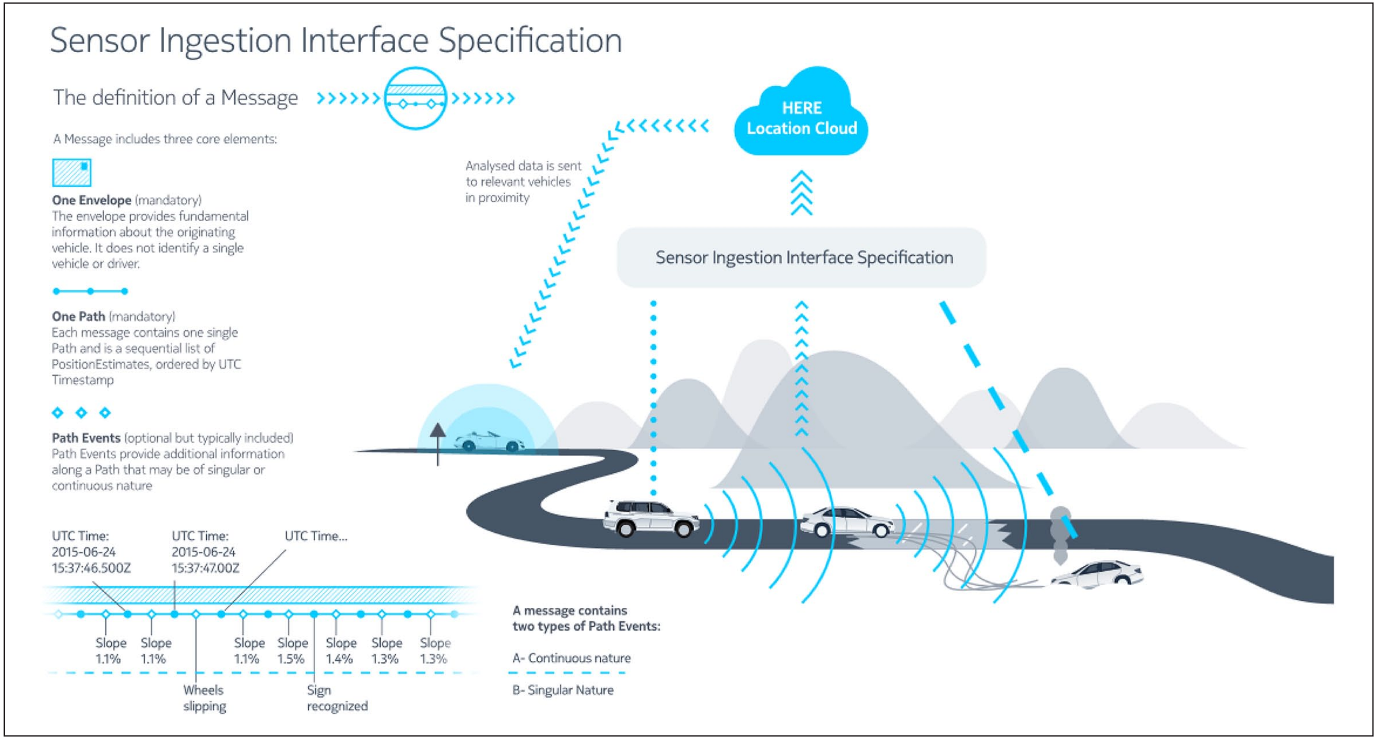
Unlike in the capture model of privacy, where protocols might determine how data are routinely collected for post hoc surveillance analysis, infrastructural surveillance of CAVs present a different issue, simultaneously defining what data are collected and how such data are implemented for the restructuring of driving activities. In other words, standards force data to *conform*, and to follow a set of instructions that subsequently *govern* their operation.

Thus, it is through the protocological nature of information systems, we contend, that infrastructural surveillance is enabled. Yet, at present, with merely connected vehicles, the standardisation of *externally* sensed data (i.e. captured by lidar, cameras), rather than *internally sensed* data (i.e. processed by a TCU) has not been reached. This had compelled some companies, such as HERE, to lead the design of an 'interface specification that defines how sensor data gathered by vehicles on the road can be sent to the cloud to updates maps on the fly' (Kent, 2015: n.p.). Externally sensed data are necessary for autonomous vehicles to navigate correctly. Without the standardisation of this data integration, they are likely to encounter serious problems: a car may miscalculate the distance between the vehicle and a cyclist riding beside it, it may pull out of a junction at the wrong time or follow the wrong road markings.

In more detail, HERE's proposed Sensor Interface Specification (SENSORIS) is a 'standardised interface for exchanging information between . . . in-vehicle sensors and a dedicated cloud as well as between clouds' (Castle, 2016: n.p.). Designed to be an open universal data format, SENSORIS is now facilitated by 28 members, including vehicle manufacturers (Audi, BMW, Daimler, Nissan, etc.), navigation system suppliers (Elektrobit, Harman, Pioneer, etc.), sensor suppliers (Bosch, Continental, Denso, etc.), location providers (HERE, Baidu, TomTom, etc.) and cloud providers (Tencent, IBM, etc.) (Figure 2). In HERE's words, SENSORIS has three goals:

> First, to enable broad access, delivery and processing of vehicle sensor data. Second, to support the easy exchange of vehicle sensor data between all players. Finally, to enable enriched location-based services which are key for mobility services as well as for automated driving. (Castle, 2016: n.p.)

Like the Internet protocols described by Galloway (2004), the SENSORIS specification is designed to regulate two kinds of traffic: flows between infrastructural nodes comprising of externally and internally sensed data and, ultimately, vehicles in everyday driving situations. What is interesting is how, in the originally produced diagram (Figure 2), sensor data



Sensor Ingestion Interface Specification

The definition of a Message

A Message includes three core elements:

One Envelope (mandatory)
The envelope provides fundamental information about the originating vehicle. It does not identify a single vehicle or driver.

One Path (mandatory)
Each message contains one single Path and is a sequential list of PositionEstimates, ordered by UTC Timestamp

Path Events (optional but typically included)
Path Events provide additional information along a Path that may be of singular or continuous nature

Analysed data is sent to relevant vehicles in proximity

A message contains two types of Path Events:

A- Continuous nature

B- Singular Nature

Figure 2. HERE's SENSORIS open specification.
Source: Kent (2015).

derived by CAVs flows *through* the open specification and *into* the 'HERE Location Cloud' before data are sent onto 'relevant vehicles in proximity'. In essence, the specification enables the aggregation of sensor data so that it can be funnelled into a 'dedicated cloud'. This, as Galloway (2004) would have it, is the 'governmentality' of infrastructure, akin to how Facebook encroached on, and ultimately replaced, open web standards. What is different here is how HERE must cooperate with, and integrate, a litany of partners, data sources, as well as data formats in order for their SENSORIS interface to become the obligatory passage point for CAV sensor data.

Distribution

What is critical, then, is how the aggregation of data combined with the standardisation of data capture, collection, storage and analysis results in the distribution of surveillance powers throughout a CAV infrastructure.

However, at present this is an 'external' capacity only made possible through schemes such as the UK's Automatic Number Plate Recognition (ANPR) system, in use since 2006, and operated by law enforcement agencies. Such systems can retrieve basic vehicle registration details for crime prevention purposes. Internal vehicle data derived from telematics cannot be accessed, beyond those that can also be determined externally (such as vehicle speed).

CAVs bring this capacity *into* the manufacturer's infrastructure. In doing so, they proliferate and distribute knowledge production throughout CAVs. This is a novel development, which opens up the possibility of countless data streams being utilised far beyond their immediate interaction with other parts within a vehicle.

Marres' (2018) discussion of the VW emissions scandal provides an interesting insight into the current distribution of knowledge within the vehicle. As she explains, software installed onto ECUs of VW models was able to detect whether the vehicle was running under test conditions. If so, the ECU would be able to change the vehicle's performance, 'dramatically reducing its emissions of CO_2 and . . . NO_x' (Marres, 2018: 9), thus enabling it to pass strict EU emissions tests. As she further argues, the exposure 'showed how the computerisation of the car makes it possible to inscribe the test conditions . . . into automotive systems – the car 'knew' when it was undergoing a test, and thereby was able to game it' (Marres, 2018: 10).

This kind of device-led or software-instantiated knowledge was made possible by the capacities of ECUs to handle specific vehicular functions *and* to relay communications to other ECUs in the vehicle. While Farivar (2018) suggests that unlike CAVs, 'older cars . . . lack . . . sensors and do not gather up . . . vast quantities of stored data', the VW emissions scandal suggests this is only partly true (n.p.). 'Older' vehicles do not lack sensors. However, one might say that they *send* vast quantities of data, without necessarily gathering up stored data. As Privacy International (2018) suggested before, 'increasingly granular data' are being collected that tracks driver behaviour (n.p.).

Herein lies the privacy distinction. TCUs – critical components in CAVs – allow these data to be sent beyond the vehicle. In the case of autonomous vehicles, they *demand* these data to be sent beyond the confines of the car itself, claiming – often without a way for an external party to challenge such statement – that without it the vehicle simply cannot be operated. Thus, this distribution incorporates forms of technological 'knowing', rather than merely a distribution of human knowledge capacities, or of data sources. This is why we differentiate this from Agre's existing privacy models that are oriented towards human action: CAVs distribute decision-making abilities to the vehicle, gifting agency to specific components, while relaying data to wider infrastructures.

Enclosure

To reiterate, drivers have often been subject to surveillance powers, such as ANPR plate registration, and capture mechanisms such as seatbelt-initiated ignition systems (Kitchin and Dodge, 2007). However, the notion of an 'autonomous' vehicle recalibrates these practices. The 'nomos' in autonomous suggests the vehicle is a sovereign power – capable of executing administrative decisions by itself.[2] As Bratton (2015) suggests, the automobile will likely become 'more and more accurate' as the 'auto' is intensified and deepened (p. 12). This has direct implications for our infrastructural surveillance concept. For Bratton, 'The Stack space is not an already given vessel into which states intervene or markets mediate or political theologies invest with myths; rather it is *generated in the confluence of platform logics*' (Bratton, 2015: 34, our emphasis). Furthermore, that 'infrastructural sovereignty . . . is produced less by formal law then by shared physical postures of political subjects *in relation to common infrastructure*' (Bratton, 2015: 21, our emphasis). How, then, is the 'autonomic' sovereign power of CAVs – this infrastructural surveillance – executed?

CAVs complicate the kind of infrastructural spaces, objects and standards that Keller Easterling (2016) discusses, subtly distinct from free enterprise zone, broadband in East Africa and ISOs, themselves exercising a unique kind of sovereignty. Frank Pasquale (2017) refers to massive digital platforms such as Amazon as demonstrating a 'functional sovereignty', different from the territorial sovereignty of nation-states. Here, such platforms amass such total power that they are largely immune from nation-state actions. But in what way do CAVs not only operate outside of statecraft, but are actively enabled by infrastructural actors? As Easterling (2016) suggests, '[i]nfrastructure space, with the power and currency of software, is an *operating system* for shaping the city' (p. I, our emphasis). While there are ways in which this metaphor is a little stretched or imprecise, her articulation that:

> As a site of multiple, overlapping, or nested forms of sovereignty, where domestic and transnational jurisdictions collide, infrastructure *space* becomes a medium of what might be called *extrastatecraft* – a portmanteau describing the often undisclosed activities outside of, in addition to, and sometimes even in partnership with statecraft. (Easterling, 2016: 15, our emphasis)

This resonates with the world of CAVs. If we return to SENSORIS, we can see how the interface specification valorises rather than limits the enclosure of knowledge. This happens not in spite of the open specification, as one might think, but because of it. The valorisation of knowledge enclosure is dependent on the acceptance of open specifications that subsequently allow for the storage (permanent or otherwise) of relevant vehicle data. Thus, the open specification allows value to be accrued (rather than strictly extracted, as is strictly the case with platforms; Barns, 2017, 2019) that is predicated on a 'no opt-out' data capture from all drivers.

Furthermore, although there is a distribution of knowledge production, this knowledge is extracted from a different infrastructural arrangement (say, ANPR), placing the CAV at the centre of data collection, and resituating enclosure. In essence, the data collected through the CAV infrastructure become infinitely more valuable (in their granularity, scope and regularity) than intermittent occasions of number-plate recognition on the highway network, for example. This is how CAVs assume a form of mobile functional sovereignty, enabled by specific interfaces such as SENSORIS, becoming the body to which other institutions must submit access requests. This is a unique, but complimentary, form of extrastatecraft.

However, returning to Farivar (2018), there are also limitations to this enclosure. The CAV is not an unshakeable sovereign power largely, but not entirely immune from the nation-state's whims. Law enforcement agencies can demand vehicle data without warrants, at least in the United States. These limitations amount to legal and technical backdoors, in which data can be freely accessed based on the public nature of the activity undertaken (driving), despite the enclosed nature of data capture, integration, storage and analysis. Here, data are indeed collected surreptitiously (akin to traditional visual surveillance), *except that they are collected as a condition of the activity (driving) itself.* In other words, CAVs are operationally dependent on the unobstructed flow of data from the vehicle. Here traditional public/private distinctions are considerably blurred, like many examples of extrastatecraft, but also decidedly one-way. Vehicle data cannot be requested from manufacturers by drivers, nor can they opt out of such data collection processes, due to their operational importance. This is the 'total' idea of infrastructural privacy we and others (Andrejevic, 2019) articulate.

In this new arrangement of infrastructural surveillance, CAVs become novel mobile, functional, sovereign objects, through which all requests must flow, while government departments are relegated to secondary, yet likely 'approved', partners. Uber's Movement initiative in which third parties are invited to use Uber trip data for urban planning (Gilbertson and Salzberg, 2017), and Waze's Beacons Programme (Rogers, 2018) through which 'low-energy microcontroller hardware' (Waze, 2019) are installed in tunnels to aid navigation where GPS cannot, are further examples of the functional sovereignty offered by CAVs. HERE, like Uber and Waze, becomes the infrastructural operator *tout court*, inverting the operational relationship between democratic political body (city, state and country) and technology provider. The condition of this changing relationship is that the non-opt-out-able data captured through the infrastructure are enclosed by default, with access granted by agreement or discretion, and offered as a subsequent, selective service. Enclosure of data is important here because it dictates the inversion of the relationship; with political bodies as mere service users, rather than executors, infrastructural operators assume greater, functional power.

Secondary also, alongside civic administrations are citizens, no longer legal subjects communicated with when issued with parking fines, speeding tickets or other such driving misdemeanours. Instead, through the aggregation of driving data, the development of new data-sharing standards, the proliferation and distribution of knowledge production and the valorisation of new forms of knowledge enclosure, CAVs assume a new kind of

Table 2. Capture versus infrastructural surveillance.

Capture	Infrastructural surveillance
Employs linguistic metaphors by means of various grammars of action.	Relies on the 'total' idea of infrastructure that is omnipresent and invisible until breaks (aggregation, enclosure).
Describes the readily apparent instrumentation that entails the reorganisation of existing (human) activities.	Reorients itself towards the facilitation of non-human actions rather than reorganisation of human ones (general).
Activities are being constructed in real-time from a set of institutionally standardised parts specified by the captured ontology.	Creates new ontologies (standards, enclosure).
Emphasises the locally organised nature of activities within particular institutional contexts.	Entails distributed organisation within infrastructural constraints (distribution).
Takes as its prototype the quasi-philosophical project of ontological reconstruction undertaken by computer professionals in private organisations.	Takes as its prototype the quasi-metaphysical 'stack' of planetary computation (enclosure).

control to which the citizen is (infrastructurally, operationally) subject. Here the driver is largely irrelevant, relegated or bypassed as the data captured in the driving of a vehicle are distributed across a larger consortium of contractual actors. In other words, it is infrastructure, rather than merely software, that takes command (Manovich, 2013).

Conclusion

In this article we have proposed a new model of privacy: infrastructural surveillance. It departs from Agre's traditional distinction between surveillance and capture, in recognition of the historicity of his original claims and subsequent changes in our technological landscape (Table 2).

For Agre, the main aim of the capture model was to remove the directed and maleficent connotation of surveillance in relation to computerisation that was being introduced into the workplaces of the 1990s. In parallel, his model pioneered other concerns that have by now become a mainstay of critical media and privacy studies: the importation of 'dividuals' and their data-bodies and data-doubles into predictive algorithms that prescribe actions (Deleuze, 1992; Langlois et al., 2009; Lupton, 2015) concomitant with their invisible biases (Noble, 2018; O'Neil, 2017).

However, it is exactly this intentionality that our model brings back. Rather than relying on the innocuous metaphor of computational data processing, we look into the totalising proposition of infrastructure as invisible and omnipresent. This becomes evident when we consider the connected and/or autonomous vehicle (CAV). Specifically, we have outlined the way it simultaneously aggregates information on a massive scale while requiring other parties – from law enforcement to component manufacturers – to agree access to such data on a granular level. Moving beyond CAVs, one can imagine a plethora of 'smart' technologies – from Alexa-like speakers to gig economy apps, embroiled in similar privacy issues. As Mark Andrejevic (2019) warns,

> Data collection on this scale initiates a cascading logic of automation. Embedded sensors automate data capture, generating quantities of information that can only be handled by automated data processing and, increasingly, automated response. While it is true that not all forms of information collection qualify as 'surveillance', the development of this sensor-permeated infrastructure enables new logics of surveillance to emerge and take hold. (p. 2)

While the capture model is predicated on the reorganisation of existing human activities in the hope of optimisation, the infrastructural surveillance model rejects the needs of the human component altogether, relegating it to an obey/discard choice. Such a model assumes the primacy of non-human actors, such as the various geographic information systems databases and sensory assemblages that make CAVs go. While historic human actions have been considered, there are no new grammars to be produced. Instead, the 'driver' is inscribed into the mechanistic script. Under the capture model, continuous and adjusting, humans may resist and alter the script. Under infrastructural surveillance, protocological power bars misuse: the only choice is to avoid using the technology altogether, again recounting escaping from within the autonomous vehicle in *Minority Report*. This inhibits efforts to 'counter-map' the spaces of CAVs as some have suggested (Alvarez León, 2019a). Moreover, it often positions the vulnerable people in society at the forefront of a privacy-or-function dilemma (Couldry and Mejias, 2019).

This protocological power is also reflected in the model's disregard for existing components. Evangelists of machine learning promise us new ways of doing things, based on previously unimaginable and inherently inhuman heuristics. If a car possesses reflexes measured in nanoseconds, if it is connected to all other vehicles on the road and the road itself, if it encompasses a cumulative driving experience of a million miles from simulations and other connected vehicle histories – what additional value does the capture of existing driving ontologies bring?

Infrastructural privacy no longer imagines the confines of a single office, the factory floor or even the corporation. Like other infrastructural projects it imagines multiple distributed networks, connected by gateways that allow them to interoperate. It is a privacy mode that requires non-localised sovereignty of extra-state powers. The double autonomous nature of the CAV exemplifies this spread: first, it limits potential participation by non-whitelisted actors, be it police or rival corporations; then, it acts agnostically towards its drivers/riders, requiring nothing of them (i.e. licencing) as long as they subscribe to the standards and provide the necessary data. It is the Brattonian stack of global computation and not the individual car manufacturer that makes such a privacy mode possible.

Ultimately, infrastructural surveillance is also a conceptual framework to appraise statements made by technology manufacturers in response to privacy advocates: 'that's just the way it works'. It pinpoints a certain common-sense logic that enmeshes usability with traceability. Mobile phones triangulate users into spatial cells, because this is how it works. Social media platforms collect troves of personal information, because this is how it works. Google incorporates evermore services that extend into our physical world, because this is how it works. Following this deterministic logic, one can criticise the *usage* of a certain media component but find it difficult to reject the operational *essence* of it.

Our framework unpacks these claims and their exact privacy ramifications by drawing on critical platforms and infrastructure studies. It affords us to be sceptical towards CAVs' – or other technologies' – value propositions, questioning this common-sense logic. If (when) CAVs begin to deliver the desired levels of safety, convenience and emissions in return for a growing reliance on sensor and behavioural data, their underlying proposition will be, you must play by our rules or not play at all. We must be ready to challenge this totalising claim and decouple the operation of digital technologies from its imposition on privacy and, by extension, civil liberties.

Acknowledgement

Both authors would like to thank the organisers of the Smart Technologies session at the Surveillance Studies Network conference in Aarhus in 2018 where we presented the early idea and to Bernhard Rieder and the Locating Media Kolloquium in Siegen for commenting on the written version.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Alex Gekker https://orcid.org/0000-0001-6042-2086

Notes

1. We thank Reviewer 1 for helping us clarify this point.
2. Thanks to Mekonnen Tesfahuney for originally alerting the authors to this etymological connection.

References

Agre PE (1994) Surveillance and capture: two models of privacy. *The Information Society* 10(2): 101–127.

Alvarez León LF (2019a) Counter-mapping the spaces of autonomous driving. *Cartographic Perspectives* 92: 5–18.

Alvarez León LF (2019b) Eyes on the road: surveillance logics in the autonomous vehicle economy. *Surveillance & Society* 17(1–2): 198–204.

Amoore L and De Goede M (2005) Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change* 43(2): 149–173.

Andrejevic M (2019) Automating surveillance. *Surveillance & Society* 17(1–2): 7–13.

Baran PA and Sweezy PM (1966) *Monopoly Capital: An Essay on the American Economic and Social Order*. 1st modern reader paperback ed. Harmondsworth: Monthly Review Press.

Barns S (2017) Visions of urban informatics: From proximate futures to data-driven urbanism. *The Fibreculture Journal* 29. DOI: 10.15307/fcj.29.204.2017.

Barns S (2019) Negotiating the platform pivot: from participatory digital ecosystems to infrastructures of everyday life. *Geography Compass* 13(9): e12464.

Batorski D and Grzywińska I (2018) Three dimensions of the public sphere on Facebook. *Information, Communication & Society* 21(3): 356–374.

Beer D (2015) Productive measures: culture and measurement in the context of everyday neoliberalism. *Big Data & Society* 2(1): 2053951715578951.

Berry DM (2014) *Critical Theory and the Digital* (Critical Theory and Contemporary Society). London: Bloomsbury. Available at: http://www.bloomsbury.com/uk/critical-theory-and-the-digital-9781441166395/ (accessed 9 June 2014).

Bissell D (2018) Automation interrupted: how autonomous vehicle accidents transform the material politics of automation. *Political Geography* 65: 57–66.

Bliss L (2018) Uber pivots to on-demand everything. Available at: https://www.citylab.com/transportation/2018/04/uber-pivots-to-on-demand-everything/557528/ (accessed 14 August 2018).

Bogost I (2006) *Unit Operations: An Approach to Videogame Criticism*. Cambridge, MA: MIT Press.

Bogost I (2007) *Persuasive Games: The Expressive Power of Videogames*. Cambridge, MA: MIT Press.

Bratton BH (2015) *The Stack: On Software and Sovereignty*. MIT Press. Available at: https://muse.jhu.edu/chapter/1754084 (accessed 24 October 2018).

Callon M (1986) Elements of a sociology of translation: domestication of the scallops and the fisherman of St. Brieuc Bay. In: Law J (ed.) *Power, Action and Belief: A New Sociology of Knowledge?* London: Routledge, pp. 196–233.

Castells M (1996) *The Rise of the Network Society* (Information Age), vol. 1. 2nd ed. Oxford ; Malden, MA: Blackwell Publishers.

Castle L (2016) HERE standard for shared car data wins pan-European backing. *HERE*, 28 June. Available at: https://360.here.com/2016/06/28/here-standard-for-shared-car-data-wins-pan-european-backing/

Clarke R (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512.

Couldry N and Mejias UA (2019) Data colonialism: rethinking big data's relation to the contemporary subject. *Television & New Media* 20(4): 336–349.

Cross GS (2018) *Machines of Youth: America's Car Obsession*. Chicago, IL: University of Chicago Press.

Deleuze G (1992) Postscript on the societies of control. *October* 59: 3–7. Available at: http://www.jstor.org/stable/778828 (accessed 12 February 2012).

Dourish P (2015) Protocols, packets, and proximity: the materiality of internet routing. In: Parks L and Starosielski N (eds) *Signal Traffic: Critical Studies of Media Infrastructures*. Urbana, IL: University of Illinois Press, pp. 183–204.

Drozdiak N (2019) Qualcomm, BMW Triumph in EU fight over connected car rules. *Bloomberg*, 4 July. Available at: https://www.bloomberg.com/news/articles/2019-07-04/qualcomm-bmw-triumph-in-eu-fight-over-connected-car-rules (accessed 2 August 2019).

Drozdiak N and Rolander N (2019) BMW, Qualcomm battle VW, Renault on connected car rules. *Bloomberg*, 17 April. Available at: https://www.bloomberg.com/news/articles/2019-04-16/bmw-qualcomm-battle-against-vw-renault-on-connected-car-rules (accessed 2 July 2019).

Durham Peters J (2015) *The Marvelous Clouds: Toward a Philosophy of Elemental Media*. Chicago, IL: University of Chicago Press.

Easterling K (2016) *Extrastatecraft: The Power of Infrastructure Space*. Paperback ed. London; New York: Verso.

European Parliament (2014) Decision No 584/2014/EU on the deployment of the interoperable EU-wide eCall service. *Official Journal of the European Union* L164: 6–9.

Farivar C (2018) Why cops won't need a warrant to pull the data off your autonomous car. Available at: https://arstechnica.com/tech-policy/2018/02/why-self-driving-cars-may-be-heaven-for-investigating-crimes-and-accidents/ (accessed 18 October 2018).

Flink JJ (1976) *The Car Culture*. New edition. Cambridge, MA; London: MIT Press.

Galloway AR (2004) *Protocol: How Control Exists after Decentralization*. Cambridge, MA: MIT Press.

Galloway AR (2006) *Gaming: Essays on Algorithmic Culture*. Minneapolis, MN: University of Minnesota Press.

Galloway AR (2010) Networks. In: Mitchell WJT and Hansen MBN (eds) *Critical Terms for Media Studies*. Chicago, IL; London: University of Chicago Press, pp. 280–296.

Gilbertson J and Salzberg A (2017) Introducing Uber Movement. Available at: https://www.uber.com/newsroom/introducing-uber-movement-2 (accessed 13 August 2019).

Hayles NK and Sampson TD (2018) Unthought meets the assemblage brain. *Capacious: Journal for Emerging Affect Inquiry* 1: 60–84.

Helles R and Flyverbom M (2019) Meshes of surveillance, prediction, and infrastructure: on the cultural and commercial consequences of digital platforms. *Surveillance & Society* 17(1–2): 34–39.

Helmond A (2015) The platformization of the web: making web data platform ready. *Social Media + Society* 1(2): 2056305115603080.

Hind S (2019) Digital navigation and the driving-machine: supervision, calculation, optimization, and recognition. *Mobilities* 14(4): 401–417.

Hind S and Gekker A (2014) 'Outsmarting traffic, together': driving as social navigation. *Exchanges: The Warwick Research Journal* 1(2): 165–180. Available at: http://exchanges.warwick.ac.uk/exchanges/index.php/exchanges/article/view/29 (accessed 23 October 2015).

Hind S and Gekker A (2019) On Autopilot: Towards a Flat Ontology of Vehicular Navigation. In: Lukinbeal C, Sharp L, Sommerlad E, et al. (eds) *Media's Mapping Impulse*. Stuttgart: Franz Steiner Verlag, pp. 141–160.

Johnson G (2012) Apple maps trying to make 'LoDel' neighborhood happen. Available at: http://gothamist.com/2012/11/23/apple_maps_is_trying_to_make_lodel.php (accessed 5 December 2012).

Kent L (2015) HERE shares how automated cars can 'heal' maps on the fly. *HERE*, 23 June. Available at: https://360.here.com/2015/06/23/here-sensor-data-ingestion/ (accessed 15 August 2019).

Kitchin R (2014) *The Data Revolution*. 1st ed. Los Angeles, CA: SAGE.

Kitchin R and Dodge M (2007) Rethinking maps. *Progress in Human Geography* 31(3): 331–344.

Langlois G, Elmer G, McKelvey F, et al. (2009) Networked publics: the double articulation of code and politics on Facebook. *Canadian Journal of Communication* 34(3): 415–434.

Lawson P (2015) The connected car: who is in the driver's seat? *British Columbia Freedom of Information and Privacy Association*, 20 March. Available at: https://fipa.bc.ca/wordpress/wp-content/uploads/2018/01/CC_report_lite.pdf (accessed 15 August 2019).

Lupton D (2015) Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality* 17(4): 440–453.

Manovich L (2013) *Software Takes Command*. INT edition. New York; London: Bloomsbury Academic.

McCormack DP (2017) Elemental infrastructures for atmospheric media: On stratospheric variations, value and the commons. *Environment and Planning D: Society and Space* 35(3): 418–437.

McQuire S (2019) One map to rule them all? Google Maps as digital technical object. *Communication and the Public* 4(2): 150–165.

Marres N (2018) What if nothing happens? Street trials of intelligent cars as experiments in participation. In: Maassen S, Dickel S and Schneider CH (eds) *TechnoScience in Society, Sociology of Knowledge Yearbook*. Nijmegen: Springer/Kluwer, pp. 1–20.

Marshall A (2017) Alphabet is trying to remake the modern city, starting with Toronto. *Wired*, 19 October. Available at: https://www.wired.com/story/google-sidewalk-labs-toronto-quayside/ (accessed 14 August 2018).

Meyrowitz J (1985) *No Sense of Place: The Impact of Electronic Media on Social Behavior*. New York: Oxford University Press.

Miller J (2015) The dematerializing interface. *Westminster Papers in Culture and Communication* 10(1): 66–80.

Miller J (2017) Mediatization of the automobile. In: Driessens O, Bolin G, Hepp A, et al. (eds) *Dynamics of Mediatization: Institutional Change and Everyday Transformations in a Digital Age. Transforming Communications – Studies in Cross-Media Research*. Cham: Springer International Publishing, pp. 203–223.

Murakami Wood D and Monahan T (2019) Editorial: platform surveillance. *Surveillance & Society* 17(1–2): 1–6.

Negroponte N (1995) *Being Digital*. New York: Alfred A. Knopf.

Noble SU (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. 1st ed. New York: New York University Press.

O'Grady N (2018) Communication and the elemental: capacities, force and excess in emergency information sharing. *Environment and Planning D: Society and Space* 37(1): 158–176.

O'Neil C (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Broadway Books.

Parks L and Starosielski N (2015) Introduction. In: Parks L and Starosielski N (eds) *Signal Traffic: Critical Studies of Media Infrastructures*. Urbana, IL: University of Illinois Press, pp. 1–28.

Pasquale F (2017) From territorial to functional sovereignty. *Law and Political Economy*, 6 December. Available at: https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/ (accessed 1 August 2019).

Plantin J-C (2018) Digital traces in context| Google maps as cartographic infrastructure: from participatory mapmaking to database maintenance. *International Journal of Communication* 12: 489–506.

Plantin J-C and Punathambekar A (2019) Digital media infrastructures: pipes, platforms, and politics. *Media, Culture & Society* 41(2): 163–174.

Plantin J-C, Lagoze C, Edwards PN, et al. (2018) Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society* 20(1): 293–310.

Poster M (2004) Digitally local communications: technologies and space. In: *The global and the local in mobile communication: places, images, people, connections*, Budapest. Available at: http://www.locative.net/tcmreader/index.php

Privacy International (2018) Case study: connected cars and the future of car travel in the digital age. *Privacy International*. Available at: https://privacyinternational.org/case-studies/118/case-study-connected-cars-and-future-car-travel-digital-age

Rankin W (2016) *After the Map: Cartography, Navigation, and the Transformation of Territory in the Twentieth Century*. 1st ed. Chicago, IL: University of Chicago Press.

Rogers A (2018) Waze lights the beacons to guide drivers through Chicago's tangled streets. Available at: https://www.wired.com/story/chicago-waze-beacons-spothero-gps/ (accessed 13 August 2019).

Sampson TD (2017) Neurolabor: digital work and consumption. In: Sampson TD (ed.) *The Assemblage Brain: Sense Making in Neuroculture*. Minneapolis, MN: University of Minnesota Press, pp. 45–74.

Schulz W (2004) Reconstructing mediatization as an analytical concept. *European Journal of Communication* 19(1): 87–101.

Star SL (1999) The ethnography of infrastructure. *American Behavioral Scientist* 43(3): 377–391.

Steg L (2005) Car use: lust and must. Instrumental, symbolic and affective motives for car use. *Transportation Research Part A: Policy and Practice* 39(2): 147–162.

Suchman L (1995) Making work visible. *Communications of the ACM* 38(9): 56–64.

Thrift N (2004) Driving in the city. *Theory, Culture & Society* 21(4–5): 41–59.

Thrift N and French S (2002) The automatic production of space. *Transactions of the Institute of British Geographers* 27(3): 309–335.

Urry J (2004) The ‘system’ of automobility. *Theory, Culture & Society* 21(4–5): 25–39.

Van der Graaf S and Ballon P (2019) Navigating platform urbanism. *Technological Forecasting and Social Change* 142: 364–372.

Van Dijck J, Poell T and de Waal M (2018) *The Platform Society*. New York: Oxford University Press.

Waze (2019) Improving tunnel navigation in cities around the world. Available at: https://www.waze.com/en-GB/beacons (accessed 13 August 2019).

Wollen P and Kerr J (2002) *Autopia: Cars and Culture*. London: Reaktion Books.

Zuboff S (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 75–89.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. London: Profile Books.

Author biographies

Alex Gekker is a lecturer in New Media and Digital Culture at the University of Amsterdam. He completed his PhD at Utrecht University, working on the relations between mapping, digital interfaces and power. He is interested in ways in which sociotechnical systems are designed to influence users, and his research touches upon quantification and datafication of society, the experience economy and interface critique. In the past he has worked in variety of media positions, as journalist, editor and spokesperson.

Sam Hind is research associate in Locating Media, at the University of Siegen. He is co-editor of *Time for Mapping: Cartographic Temporalities* (Manchester, 2018) and co-author of *Playful Mapping in the Digital Age* (Institute for Network Cultures, 2016). He has published in the *Living Maps Review, The Cartographic Journal* and *Mobilities*. He completed his PhD in Interdisciplinary Studies at the University of Warwick in 2017 and was previously research assistant on the *Playfields* project. His main research interests include digital navigation and playful methodologies.