CRIMINOLOGICAL ENCOUNTERS

Vol 5(1) 2022
ISSN 2506-7583
DOI 10.26395/CE22050118

On Tesla: Balancing sustainable car connectivity, silent lethality and luxury surveillance

Yarin Eski
Vrije Universiteit Amsterdam
y.eski@vu.nl

Marc Schuilenburg
Vrije Universiteit Amsterdam / Erasmus University Rotterdam
m.b.schuilenburg@vu.nl

Keywords: Tesla, luxury surveillance, autonomous cars, aspirational class, big data

Abstract:
This article analyses the increasingly influential role of tech companies in designing and deploying smart surveillance in private vehicles. Using the case of Tesla, a company that makes optimistic promises and has a hopeful vision for more sustainable electric cars by decreasing the ecological footprint, the article will discuss the problematic aspects of artificial intelligence, big data and algorithms for total surveillance by private companies. In particular, light will be shed on the issue of discourses on sustainable and smart vehicles that dim the light on the problematic aspects of luxury surveillance. As will be made clear, Tesla's green and lean – aspirational – ambitions through different technological and surveillance advancements revive old forms of control and introduce a new set of power/knowledge relations. Beyond the question of privacy and personal data harvesting, this article discusses the wider social and political consequences of smart car luxury surveillance by private companies such as Tesla.

Introduction

"Tesla update activates the in-car camera for driver monitoring" is the headline of a recent article on AutoBlog's website (2021). With optimistic promises and a hopeful vision surrounding the discourse on these smart vehicles, it can be easy to lose track of how the embedded smart surveillance in automobiles – powered by big data, artificial intelligence (AI) and algorithms – not only expands the possibilities for current control but also introduces a new set of (problematic) power/knowledge relations. Although Tesla has received much praise for its electric cars, it was also awarded the 2020 German Big Brother award for the collection and storage of sensor data in and around their cars.[1] In this article, we analyze the increasingly influential role of tech companies in designing and deploying smart surveillance in private vehicles. In particular, we focus on tech pioneer Tesla and its big data and AI-driven autonomous vehicles that analyze and influence the behavior of its driving customers.

To understand this set of "luxury surveillance" (Gilliard & Golombia, 2021) and (soft) power relations, we first deliver the context of the current practice of surveilling consumers. Although consumer surveillance has been approached in numerous ways, from a "modular" to a "political economic perspective" (Pridmore, 2012), little research has been carried out on the way private vehicles have become "fortified" into tools of total surveillance. To conceptualize this historical development, we will look at the continuum ranging from the military tank to the private vehicle to analyze how private cars have become militarized in recent decades. We then focus on the way tech company Tesla is building and advertising digitally secured and controlled vehicles, including cars such as the Model Y and the Cybertruck, which Musk called a "futuristic battle tank." Beyond the question of privacy and personal data harvesting, we analyze in the conclusion the wider social and political consequences of smart car luxury surveillance by private companies: How does this form of power work? What type of power are we discussing? And who benefits from it? In other words, how do we make sense of Tesla's ambivalence resulting from its "lean and green" approach to building a more environmentally friendly world and a brighter future by creating sustainable car mobility (Tesla, 2021a) while using cutting-edge privacy penetrating surveillance technologies that reveal Tesla's other ambitions (Cooke, 2021)? To address these questions, our conceptual–theoretical lens will first be provided to develop an understanding of luxury surveillance and its consumption by today's aspirational class.

Conceptualizing luxury surveillance of the aspirational class in the digital consumption society

Corporate surveillance

The enforcement of security using surveillance technologies was once a primarily vertical affair in which the state enjoyed a monopoly. However, an increasing number of parties other than the police have become active and deploy all types of surveillance technologies, from WhatsApp groups patrolling the streets of their neighborhoods to private security at airports using biometric technologies to monitor and identify passengers (Bayley & Shearing, 1996; Johnston & Shearing, 2003; Marx, 2016; Schuilenburg, 2015). In this new framework, the emergence of surveillance technologies takes place "above" (transnational actors), "below" (in the community), and otherwise "beyond" the state (corporate actors; cf. Loader, 2000).

One of the most persistent visions of a safe and secure society by corporate actors concerns the notion of a "smart home." The use of interactive technologies to make homes smarter has become a global narrative that promises to improve resource efficiency and decision making, increase leisure

1 See: https://bigbrotherawards.de/2020/mobilitaet-tesla (Visiting date: accessed March 10, 2022).

time, and help residents to feel safe (Maalsen & Sadowski, 2019; Sadowski et al., 2021). Some argue surveillance technology has made smart homeowners become self-managing prisoners in their own privately owned panopticon where our household objects invisibly monitor us, turning us into household-monitored objects (cf. Edenius, 2006; Gilchrist, 2017; Jonsson, 2006). The unobtrusive surveillance relies on ubiquitous computing that is purposefully designed to make computing and other smart surveillance technology vanish into the background while advancing mobility (Lyytinen & Yoo, 2002; Weiser, 1991).

Research on of how private life is entangled with the rise of smart surveillance is rapidly increasing (Garfunkel, 2021; Kitchin 2014; Perzanowski & Schultz, 2016; Rosenblat et al., 2014). For example, the (digital) work floor is becoming saturated with private surveillance solutions and technologies, making it easier to manage workers (Buckey, 2019, 29). Researchers problematize such surveillance as it may have "removed autonomy, discretion, and prestige from workers and allotted it to a managing elite," assuming "there isn't a point of mutual consent amongst all parties involved," while "the boundaries of what is possible stretch uncomfortably into the blurry terrain of what is permissible and what is considered a violation" (Rosenblat et al., 2014, 2, 15). Much like in the (digital) workplace, in the domain of (large) property ownership, corporate surveillance manifests itself in real estate. In Israel, private owners of high-rise luxury condominiums are seduced to integrate high-tech surveillance equipment into their buildings to make renting them more appealing (Garfunkel, 2021). In addition, (online) consumption and consumer autonomy, discretion, and prestige also appear to be affected by corporate actors that aim to control their (software-enabled) goods (Perzanowski & Schultz, 2016). This happens physically, as concrete "[e]veryday objects are being replaced or supplemented by information enabling a 'digital economy' structured around interconnected devices and data [that] holds immense promise" (Perzanowski & Schultz, 2016, 191). However, such promising interconnectedness creates a "power to redefine or even eliminate the notion of personal property" and that "puts us all at risk of exploitation," as we increasingly tend to lose control over our lives by entrusting them "to a handful of private companies" (Perzanowski & Schultz, 2016, 192).

This means that nearly every aspect of life in which technology has entered the domestic space has seen the introduction of a smart alternative, from smart lighting systems and smart thermostats to smart locks and smart doorbell cameras. In addition, the implementation of smart technologies is presented as a solution to all kind of "catastrophic events" (Pali & Schuilenburg, 2020; Sadowski & Bendor, 2018, 2020) that we face now and will face in personal environments, from the office and hotel rooms to our houses and cars.

The aspirational class

The fact that people are willing to pay for smart surveillance technologies leads to a new cultural class with its own self-sustaining social stratification; this has been referred to as the emergence of an aspirational class (Currid-Halkett, 2017; Deka, 2021). The members of the aspirational class are consumers whose decision making establishes norms that appear as inclusive, green, and, thus, admirable, but in doing so, they have a far more malicious impact on society than previous elites have had (Currid-Halkett, 2017, 185). At the same time, they remain comfortably numb and incapable of trying to "imagine (let alone solve) the pervasive problems of their poorer fellow citizens" (Currid-Halkett, 2017, 189). Such consumer aspirationalism keeps people "wilfully ignorant that many of these decisions, veiled in morality, are practical and realistic outcomes of socioeconomic position" (Currid-Halkett, 2017, 196).

Making it luxe to have an organic, sustainable and fair-trade lifestyle is a growing priority for the aspirational class, and the technological surveillance of it is called "luxury surveillance", for which

"[p]eople pay for and whose tracking, monitoring, and quantification features are understood by the user as benefits they are likely to celebrate" (Gilliard & Golombia, 2021). It accommodates the surveillance creep (Lyon, 2003) because its dataveillance introduces "seemingly benign, useful and convenient technological artefacts" with perverse effects (Coulthard & Keller, 2010, 3). Such luxury surveillance "acts like a perfectly automated and optimised maternal ecosystem [that] is confronted by the reality of households as imperfectly chaotic and haphazard social spaces" (Sadowski et al., 2021, 12). This ecosystem makes luxury surveillance and the development and marketing of technology enabling it "a story of capital and profit" (Sadowski et al., 2021, 12). It brings forward certain technologies proving to be the "'best' from the point of view of the producer [but] not necessarily 'best' from the point of view of the consumer […] not because one [technology] was technically better than the other, and not even because consumers preferred one machine (in the abstract) over the other" but because these are very "very large, very powerful, very aggressive, and very resourceful companies," and their competitors are not (Cowan, 1983, 143–144).

The rise of tech-moguls in the information economy

Corporate actors, in particular 21st century tech companies, have great interest in the development of luxury surveillance and the governance of and by software-enabled smart products through software licensing and intellectual property law, leading to and further sustaining a wide range of problematic, sometimes discriminatory, treatment of its customers as well as by its customers (cf. Perzanoski & Schultz, 2016; Tusikov, 2019a; Van Dijck, 2014). Tusikov (2019b) speaks of "techno-regulation," a type of design-based regulation in which the employment of technology shapes the behavior of consumers. Previously known as "titans of wealth" (Fridson, 1999), such as the Buffets and Rockefellers, the list of titans today includes some of the richest and most influential people who have ever lived on this planet. The "titans of wealth 2.0" make their profits from software development and other technological digital solutions (Moran, 2020; Park, 2020). They are known as "easy-accessible pioneers" that aim to technologically improve our lives while making their billions by their invisible but omnipresent infiltration into everyday activities (Murtola, 2018; Solomon, 2011).

This has led to the rise of platform or surveillance capitalism that is run by a few powerful digital platforms that have become almost entirely reliant on big data and AI, ranging from Airbnb and Deliveroo to Uber (Srnicek, 2017; Zuboff, 2019). Merely focusing on solving problems with digital solutions vis-a-vis digital solutionism has led to a strong demand if not hunger for applications such as Facebook, Instagram, or Google Maps, which offer us freedom and joy as well as problem-solving capacity to deal with our social life and its multifaceted challenges (Magalhães & Couldry, 2021). Accordingly, if you possess a strong sense of algorithmic knowledge and its applicable use in everyday life and you manage to monetize it, you can relatively quickly become a billionaire and a powerful actor on the world stage.

Being a tech billionaire means, among other things, that you act as a philanthropist on that same world stage by giving extremely large donations to charity which rather seems to sustain a perverse type of philanthrocapitalism that "might exacerbate the same social and economic inequalities that philanthropists purport to remedy" (Eikenberry & Mirabella, 2018, 44). The portrayal of yourself and your company as aiming for a better world through smart technology and philanthropy is incarnated, at best, by Elon Reeve Musk and his companies Tesla Inc. and SpaceX (Moskowitz, 2012; Vance, 2015). Particularly interesting and relevant for this article is how Tesla is using luxury surveillance to build, market, and hive data from militarized vehicles and their drivers. A clear example is the all-electric, battery powered, armored Cybertruck, which Musk called a "futuristic battle tank – something that looks like it could come out of Blade Runner."[2] In order to understand both the mi-

2 See: https://auto.hindustantimes.com/auto/cars/elon-musk-calls-cybertruck-a-futuristic-battle-tank-has-a-plan-if-it-flops-41596511158518.html (accessed March 10, 2022)

litary metaphors that are used ("battle tank") and the way Tesla vehicles have become fortified into tools of total surveillance, a few words on the evolution of such private car fortification is required as seen from the historical perspective of vehicle militarization; that is, how have cars turned into "driving castles" with smart surveillance and networked security systems which increasingly rely on state-of-the-art "thinking" algorithms and big data to support decision making and to predict "risky" patterns or situations on the road? In a bid to answer this question, it is instructive to consider the surveillance continuum from the military tank to police cars.

From the military tank to the police car: a surveillance continuum

From a historical perspective on cars, little research has been employed on the way private vehicles have become "militarized." An exhaustive catalogue of the surveillance technology that has turned vehicles into "driving panopticons" is beyond the scope of this article, but a starting point for a better understanding of the nexus between surveillance and vehicles is the military tank. Virilio (1994, 41) writes that the tank was the first "fortification on wheels. With its tens of tons, the tank could be identified as an iron casemate." Apart from its ability to be an offensive weapon, the original design of the tank functioned as defensive architecture, combining the "inventions of high-strength steel and the internal combustion engine, all in service of overcoming barbed wire, trenches, and machine guns" (Mills & Mills, 2014, 6). Currently, military tanks are equipped with a range of technological innovations, with surveillance applications in support of infantry house-to-house clearing operations. According to Wilson (2012, 273), "military vehicles are equipped with night vision and video facilities that facilitate combat being monitored in real time and for the remote guidance of munitions." The US tank M1A2 Abrams, for example, allows the crew to scan the urban battlefield through thermal viewers, to acquire targets, and to move with the help of an inter-vehicular information system (Wright, 2001, 409).

Although the tank realized its true potential in the Second World War, the concept of an "automotive fort" (Virilio, 2006, 78) still impacts "social consciousness, art, political discourse and issues of morality and peace-making" (Liebenberg, 2015). Numerous authors have indicated the foundational importance of the surveillance technologies of the military tank on the way policing is now employed in public space (e.g., Dandeker, 2006; Graham, 2011). In order to win urban wars, police cars are equipped with a plethora of electronic and computerized devices for crime control and prevention, from cameras mounted on or in a police vehicle (e.g., license plate recognition) to a rugged in-vehicle network video recorder (NVR) system targeted for surveillance, recording, and video analytics. Ericson and Haggerty (1997) were the earliest scholars to argue that the activity of policing was moving away from order maintenance. Instead, policing is now focused on risk management in line with the imperatives of the "risk society" (Beck, 1992) and associated insurance discourses (Feeley & Simon, 1992). This was manifested in police patrol cars, which became "mobile offices and technological laboratories, wired with voice radios, cellular telephones, computer-assisted dispatch terminals, laptop computers, radar, video cameras, remote microphones, breathalyser equipment, fax machines, printers, and vehicle locators" (Ericson & Haggerty, 1997, 135).

The use of a battery of sophisticated sources of surveillance technologies in patrol cars is presented in neutral terms since they promise to bring better decisions more quickly and more insights in complex urban realities through informative and seamless interfaces. In recent literature, however, critical scholars have argued that these surveillance technologies are anything but morally neutral and are rather normative and political and that their use in urban practices has important legal, political, and social implications (ACLU, 2014). An interesting illustration is the transfer of surplus armored vehicles from the US military to the US police as part of police crowd control, particularly against political mobilization in communities of color, such as during the protests in Ferguson af-

ter the death of Michael Brown (Gordon, 2019). Like the military tank, the armored police vehicle makes "constructing vehicle barricades – lines through urban space that are rapidly deployed and easily manoeuvred" (Denman, 2020, 1147) possible. Scholars warn of a "boomerang effect" (e.g., Denman, 2020; Foucault, 2003; Gregory, 2004; Graham, 2011) of the mechanisms of "power," establishing new forms of domination and knowledge from vehicles deployed in both colonial occupation and urban crowd control.

In a context marked by a decrease in the reach and power of the police institution and the rise of corporate actors in the delivery of safety and security, the question becomes relevant as to how the ascribed militarization process also affects the design of private vehicles. In the following paragraph, we focus on the way Tesla is building and advertising their digitally secured and controlled electric vehicles, including cars such as the Model Y and the Cybertruck. How do these cars revive "old" forms of surveillance and introduce a new set of power/knowledge relations?

The Tesla case: visible lethality, invisible data-docility, distant captivity

On the Tesla website, Musk presents "The Mission of Tesla" (Tesla, 2021d):

> Our goal when we created Tesla a decade ago was the same as it is today: to accelerate the advent of sustainable transport by bringing compelling mass market electric cars to market as soon as possible. […] In order to get to that end goal, big leaps in technology are required, which naturally invites a high level of scrutiny. That is fair, as new technology should be held to a higher standard than what has come before. However, there should also be some reasonable limit to how high such a standard should be, and we believe that this has been vastly exceeded in recent media coverage.

According to the car industrial sector, Tesla has managed to make the electric car a desirable vehicle and has thus made environmental awareness a stylish and consumable ideal (Macri, 2018). The cars' performance has been described as "outstanding" or "electrifying," and it comes at a high price; for example, the Tesla Model S is priced between $100,000 and $150,000 (AutoExpress, 2020). Tesla is considered to be far ahead of its competitors in the advancement of the connectivity of a car, with more older car brands having a hard time keeping up (Weiss et al., 2020). In particular, Tesla is seen as avant-garde (PR Newswire, 2014; Sakamoto 2014) in respect to developments in the last decade on what is interchangeably referred to as "the connected car experience" or "car connectivity" developments. In 2020, Tesla won an award for pioneering the advancement of futuristic technology features built into their cars, living up to their promise "that the car of the future will be autonomous, connected, electric and shared" (EVANNEX, 2020).

Kick-started by General Motors, Tesla wants to champion making today's and the future's vehicles as "connected" as possible (Auto Connected Car, 2014), striving to be victorious in the merger of the platform economy and car industry by wirelessly advancing the exchange of information with the vehicle manufacturer, third-party service providers, users, infrastructure operators and other vehicles (A. Schmidt et al, 2021; Teece, 2018). In this way, Tesla desires to set the standard for increased comfort and convenience for customers while portraying itself as achieving sustainability goals and establishing road safety by reducing fuel consumption and facilitating traffic management and parking (A. Schmidt et al., 2021). Also, Tesla presents itself as the main market pioneer and dominator by aiming to fully implement the first three of the four new technological car paradigms: (1) electric vehicles, (2) autonomous vehicles, (3) connected cars, and (4) transportation-as-a-service (TaaS; Teece, 2018).

The Tesla vehicle fleet comprises a few on-sale models and other types, each of which have a num-

ber of different versions: Model S, Model 3, Model X, Model Y, and the Cybertruck (Tillman, 2021). These models are generally considered as too unavailable for the wider public and are therefore considered elite; only the predominantly upper(-middle) class can afford Tesla cars (Taffel, 2018). Hence, driving Tesla's electric cars appears to be an elitist activity, which is one of the major critiques of the company (Crothers, 2015; Kester et al., 2020; Sovacool et al., 2019). Despite Musk's claim of openness to critique in a realistic manner, if (technical) scrutiny is given by another party or the company senses it is being affected by defamation, there is a risk that Tesla might sue (cf. Lambert, 2021). This occurred with the TV program Top Gear when a complaint of libel was made against the TV makers after one of the presenters, Jeremy Clarkson, gave a "typically provocative review of the Tesla Roadster car" (Halliday, 2013). Thus, Tesla may present itself to be provocative, controversial, and open to feedback, yet when the company's name and reputation is provoked, the company goes on the offensive. Moreover, while Tesla wants to be open to critique, reflective and rather controversial in its actions, there are other issues about Tesla's businesses in relation to driver's physical safety and safeguarding of a driver's privacy.

1. Being unsafe, visible death, and destruction

Two categories of inherent dangers in Tesla cars have surfaced over the last few years related to the way it is building and advertising digitally secured and controlled vehicles: (a) lack of safety, visible death, and destruction; and (b) hidden privacy-related threats, including invisible detectability, docility and data-collection. Regarding Tesla cars' visible lethality and injury, there are several instances that have become increasingly problematic. Ranging from "bugs in the system" that pushed Tesla to recall 29,193 of the cars they exported to China "due to technical issues that impose safety risks" (Gasgoo, 2020) to a Dutch cab company called Bios-Groep that took Tesla to court and demanded 1.3 million euros in damages because of approximately 70 Tesla cabs at Amsterdam's Schiphol Airport with on-going technical defects and poor service (Electrive, 2020). While Tesla is interested in delivering a sustainable and safe car connectivity experience, it appears to encounter to a certain extent challenges in delivering safe cars (Canellas & Haga, 2020; B. Schmidt, 2020. Research has indicated that the quietness of hybrid and electric cars in especially busy metropolitan areas causes risks to pedestrians or cyclists who are overwhelmed by noise coming from non-hybrid and non-electric cars (Stelling-Kończak et al., 2015).

It is especially Tesla owners who are part of "the big white middle class" with a high household income that reside in those noisy urban areas (cf. Fortuna, 2019; Nygaard, 2019; Stillerman, 2020). Despite their aspirationalist consumer drift to become more environmentally friendly (Currid-Halkett, 2017), they pose new risks by driving Tesla cars silently and softly with negative outcomes. These contradictory effects stand in stark contrast to Tesla's appearance of being greener and cosmopolitan, as is further reflected in its aspirations to produce cobalt-free batteries for their electric vehicles because cobalt is mined under conditions that often violate human rights (Crawford, 2021; Ribeiro & Tang, 2020). However, cobalt forms the very safety element in the battery, and by reducing it, the life cycle of the battery would be reduced (Chen, 2018). This means that cobalt-free batteries sound very welcome if they can reduce human rights violations in the Democratic Republic of Congo where cobalt is primarily mined; their practical effect, however, involves several risks for Tesla's electric car owners.

The most lethal aspirations comprise consumer deception through Tesla's autopilot ambitions (Beene, 2018; Hess, 2020). The website www.tesladeaths.com registers every known Tesla-related deadly accident. From 2013 until the time of this writing, the website states that 240 people passed away in a Tesla-related accident, of which the most were in the US, followed by Germany and then China. The year 2021 had the highest rate so far with 56 Tesla-related deaths. Of the 240 Tesla-related deaths since 2013, 23 of them were claimed to have happened because of Tesla's autopilot

function, and 11 deaths have been verified as such according to the website. The most recent Tesla autopilot-related death involved a complete stop, or "phantom braking," of a Tesla Model 3 on an interstate highway, which caused a three-car crash and killed the driver (Levin, 2022). The Norwegian Road Traffic Information Office shows that Tesla cars crash twice as often as regular cars (Honningsvåg, 2019). The Highway Loss Data Institute (HLDI) discovered that Tesla cars have two to four times more non-crash fires than the average car, with damages up to seven times higher (HLDI, 2018). A comparison between Tesla's autopilot fatality rate with the general driver fatality rate as calculated by the Insurance Institute for Highway Safety (IIHS) indicates that a Tesla is three times more dangerous than the average passenger vehicle (Staver, 2021). The concern over the advertising by Tesla of its autopilot function as safer than non-autopilot driving is growing because researchers are calling for more driver monitoring (Templeton, 2020).

Musk argued on Twitter that the autopilot mode cannot be blamed for fatal crashes (BBC, 2021). Tesla's autopilot is presented as safe, but as a disclaimer, Tesla also states that the driver still "is both literally and figuratively in the driver's seat, and is responsible for the safe operation of the car even when self-piloting technologies are operating" and a driver's "inattention can be fatal" (McAfee & Brynjolfsson, 2017, 67). The argument often given from autopilot car manufacturers is that a driver's overconfidence "in the abilities of the self-driving system after seeing it operate effectively in many previous instances can lead to paying less and less attention to the road" (McAfee & Brynjolfsson, 2017, 67). This means it is the driver's responsibility, not Tesla's. However, this has been considered as consumer deception with very lethal consequences (Levine and Simpson, 2018; Torchinsky, 2018). The Centre for Auto Safety and Consumer Watchdog, two consumer advocacy groups, put in a request to the US Federal Trade Commission in 2018 "to investigate Tesla for 'deceptive advertising and marketing practices and representations' about Tesla's Autopilot semi-autonomous driving system" (Torchinsky, 2018). The request states that deaths and injuries are an example of Tesla's deceptive marketing to consumers, which makes consumers believe the autopilot function is safer than it actually is; combined "with Elon Musk's public statements […] it [is] reasonable for Tesla owners to believe, and act on that belief, that a Tesla with Autopilot is an autonomous vehicle capable of 'self-driving'" (Levine and Simpson, 2018, 1).

Exposure to such critics is a risk for Tesla. Therefore, the company seems to make many efforts to minimize such exposure, or at least relativize (its own accountability for) incidents. For example, the National Transportation Safety Board (NTSB) discovered that a Tesla driver who crashed his vehicle into a fire truck in January 2018, was eating and drinking coffee while using the autopilot function. Tesla had its own investigation claim that the driver was on his phone, which was subsequently denied by the driver (Tangermann, 2019). In regard to manufacturing glitches, battery longevity problems. and other types of safety issues, there have been several investigations by governments that have always been counter-investigated by Tesla itself (e.g., Shepardson, 2020). The question then arises as to when and to what extent Tesla will be as concerned with the damages done to its drivers as it is with damages done to itself.

2. Invisible detectability, docility, and data collection

Promising safety and security, Tesla designs its cars and its car connectivity experience with pervasive techniques of control and surveillance (Ahmad & Khan, 2019; Cooke, 2021; Feldstein, 2019). Having embraced a concept of luxury surveillance, Tesla develops vehicles in relation to their electric energy source and drivers, with the help as well of AI and big data. This means that Tesla does not consider a vehicle in isolation but in relation to its ecological footprint (Ahmad & Khan, 2019, 18). Tesla persistently integrates highly intrusive smart surveillance technologies into its autopilot cars through AI and machine learning (Ingle & Phute, 2016). By using IoT technology, that is, an Internet of Things (IoT)-powered mobile surveillance, Tesla turns its cars with their built-in cameras

into moving AI-powered driving surveillance forts that can structurally spot, track, and store license plates and faces, all to make Tesla car owners aware of utilitarian forms of danger such as thieves and vandals (Feldstein, 2019, 23–24).

The outward luxury surveillance is complemented by built-in driver attention monitors, which is an inward surveillance safety system of a vehicle that assesses the driver's alertness, and it warns drivers if they need to hit the brakes (Smith et al., 2008). The inward luxury surveillance is enabled by infrared sensors that monitor a driver's attentiveness through facial recognition. If attention steers away from the road (inward monitoring) and the car detects an outside dangerous situation (outward surveillance), the driver is warned by flashing lights, warning sounds, and other techniques, and if the driver remains inactive, an autonomous emergency brake will be utilized by the vehicle (Dong et al., 2010; Tusikov, 2019b). This has (been explained as having) prevented Tesla car driving customers from causing accidents, for example, when they were detected to have been looking down on a phone too often while driving (Cantu, 2021). The inward monitoring system also includes the possibility to detect the specific size of passengers, for example, to customize the airbag. It can also detect small movements, such as of a normally breathing baby in the backseat who has been left behind (Bolca, 2019; Hijink, 2021).

What both the inward and outward luxury surveillance produce is a very "large amount of data created by its fleet of vehicles and the Autopilot sensor suite on those vehicles" (Lambert, 2018, online source; Ahmad & Khan, 2019, 18). That fleet has integrated a "kind of universal 'hive mind' which share[s] data about the roadside objects they pass" that "helps the company build over time an understanding of which objects are permanent (they're the ones passed in the same spot by many different cars) and thus very unlikely to run out into the middle of the road" (McAfee & Brynjolfsson, 2017, 79).

The in-car camera and their tracking capacity have raised several concerns about privacy (Barry, 2021). The models 3 and Y "are equipped with a Cabin Camera that is located above the rear-view mirror and turned off by default," which can record a short video clip to be "shared with Tesla following a safety event such as a collision or an advanced emergency braking (AEB) event" (Tesla, 2021b). In addition, the steering wheel feedback and capacitive touch sensors are used to capture whether a driver is indeed paying attention or not. For example, this is done to determine whether to disable certain features if drivers have their hands off the wheel for too long (Lambert, 2017). It is said that the sensory equipment and the driver-facing camera are installed to protect the driver and that it supports Tesla's development of "safety features and software enhancements" (Lambert, 2017, online source). This means that the "footage recorded from these cameras after the fact [are a] part of [Tesla's] research into self-driving technology" (Barry, 2021). Despite the fact that Tesla's website states such footage is not checked against a driver's 17-digit Vehicle Identification Number (VIN) or other information that can identify a driver (Tesla, 2021c), it is always possible "that insurance companies, police, regulators, and other parties in accidents will be able to obtain that data," according to John Davisson of the Electronic Privacy Information Center (EPIC; Barry, 2021). Based on the European Union's General Data Protection Regulation (EU GDPR), the European Data Protection Board (EDPB) has argued that the GDPR's rules on processing personal data in the context of connected vehicles and mobility-related applications, there should be a delete button installed in the dashboards of such driver data-collecting cars (EDPB, 2020). This has to do with the fact that almost all the information gathered is sensitive private data; the driver as a consumer ought to know what data is being collected and for what purposes and should always be able to delete it at any given moment (EDPB, 2020). Tesla has stated it welcomes those EDPB guidelines but has responded with questions and unasked for recommendations (Tesla, 2020):

[W]e already provide vehicle owners with a mechanism to factory reset their settings and preferences directly from the vehicle's interface at any time. The EDPB [guidelines document], however, prescribes a specific method for reaching this objective in stating that "[…] a profile management system should be implemented inside the vehicle in order to store the preferences of known drivers and help them to change easily their privacy settings anytime" (emphasis added). The method for reaching this objective should not be limited to implementation inside the vehicle's interface alone, which does not allow for continued innovation of connected vehicles in this area (idem. 5 – emphasis added by authors).

Tesla then moves onto their recommendations to the EDPB and suggests that the EDPB Guidelines, in particular paragraph 88 on the rights of the data subject, would become clearer if the following were stated: "To facilitate settings modifications, a profile management system should be implemented ~~inside the vehicle~~ [to be easily accessible by the user] in order to store the preferences of known drivers and help them to change easily their privacy settings anytime" (EDPB, 2020, 6). It would also be beneficial, Tesla argues, if it is the driver's own responsibility to make their passengers aware of how the individual driver's privacy preferences are set (EDPB, 2020, 7). This suggests that if drivers forget to mention the way in which the privacy preferences are set, their passengers would unknowingly let their data double be created through the in-car detection technology. That would also mean that Tesla can still use such data for "safety development purposes" but cannot be held responsible if a passenger would bring the company to trial.

Actually, Tesla itself can use and has used such data not only for their safety research but also for their benefit in legal cases in which Tesla has blamed drivers after a crash for being inattentive while using the autopilot. Data, such as footage, has been used to prove in court that a driver was distracted (Barry, 2021). This raises several legal and ethical concerns about the terms or agreements under which the software installed by Tesla is used (cf. Perzanowski & Schultz, 2016). Are cameras on board installed merely to advance driver safety, as Tesla asserts, or are they there as well to establish the company's plausible disclaimability? Van de Weijer raises awareness about not being too naive as a Tesla driver:

Such a car simply knows everything about you, what you're doing, where you work, where your mistress or mister lives. […] The new Tesla has eight camera's, they see everything. Theoretically spoken, with access to one percent of the cars, you can already map the whole world real-time (in: Naafs & Wijnen, 2020).

In short, a Tesla car gives rise to a digitized and globalized lightness of being (Bauman, 1999), of being environmentally friendly while having the ability to be environmentally anywhere, at any time – both virtually and physically. At the same time, the universal hive mind makes it possible to control the drivers by turning them into data-gathering and data-doubling tools, as Bauman and Lyon (2013) have observed regarding liquid surveillance in general. Potentially on a global scale and more swiftly than ever before, a Tesla car may appear to set its drivers free, but what it really does is use its drivers while "including 'free choice' in the[ir] marketing strategy, or more precisely, rendering servitude voluntary and making submission be lived through as an advance in freedom and testimony to the chooser's autonomy" (Bauman & Lyon, 2013, 115). And if something goes (lethally) wrong, Tesla's initial reaction is to defend itself instead of its drivers. Altogether, a narrative of visible lethality, invisible data-docility and distant captivity surrounds Tesla, which requires further empirical scientific studies into Tesla's intentions and its unintended consequences and harm.

The panopticar? A conclusion on power, luxury surveillance, and the aspirational class

The private car has been, like other modes of production, subject to constant changes over time, both in terms of markets and technological improvements. This means that the car narrates something about current society, culture, and identity to the extent that a buyer projects its (social class and related) ambitions onto a car (Packer, 2006; Timmer, 1998). According to Sørensen and Sørgaard (1994), the car driver's experiences have symbolic, cognitive, and practical aspects integrated into a style of driving and an identity. This has also been observed in regard to the ownership of sustainable electric cars (Axsen et al., 2018; Ingeborgrud & Ryghaug, 2017). However, what meaning is given and what sociological insights into such meaning reveal remain scarce in surveillance and policing studies.

For many people, just like their home, one's car is one's castle: a free and private environment that is increasingly turned into an electronically fortified personal space. This space has become a luxury item because it is, among other things, drenched in expensive smart surveillance technologies. In analyzing the increasingly influential role of tech companies in designing and deploying smart surveillance in private vehicles, we have advanced the notions of "luxury surveillance" and "militarization" as two ways to understand how vehicles are now increasingly turned into driving panopticars, using smart surveillance to support decision making and to predict risky patterns or situations on the road. A fitting example is the way Tesla's data-driven business model is revolutionizing autonomous cars, using luxury surveillance to document the actions by all active subjects within their vehicles. In wanting to deliver safety and security, drivers are continuously watched and assessed. Through in-car monitoring systems, Tesla collects location data and the car's personal settings. As has been shown, the tech company also tracks the speed, mileage, and where and when the driver charges the battery. It knows exactly when the autopilot is engaged and whether the driver has his or her hands on the wheel.

As luxury surveillance takes on a dominant role in private cars, it becomes increasingly important to understand how this form of surveillance reshapes power/knowledge relations from disciplining and normalization to the prediction and optimization of the behavior of drivers of the cars. Playing on the term "algopticon" (Jamil, 2019) to refer to the way the panopticon's architecture of power is reproduced in the era of surveillance capitalism, we stress that it is important to realize that luxury surveillance expands and underpins already existing sovereign and disciplinary power mechanisms. The example of Tesla's autonomous cars makes this clear. It can be argued that in surveillance capitalism, (tech-)billionaire companies such as Tesla are the new holders or the expression of classic sovereign power, clearly reflected in how Tesla uses the data from their in-car monitoring systems for their benefit in cases in which Tesla drivers were inattentive while using the autopilot. This means that Tesla cars can be theoretically considered as soft power incarnated into raw hard power, and we may even speak of "algorithmic violence" (Bellanova et al., 2021; Safransky, 2020), in this case "corporate algorithmic violence," that can be committed by a corporate actor and inflicted upon drivers through their car's connectivity but also upon "suspicious persons" outside of the car. Finally, despite wanting to present itself as a progressive and humanitarian company striving towards a smarter, greener, and less noisy connected car experience, this article has shown such admirable business strategies of Tesla come at a dear price, both in terms of physical hazard and of privacy-violating technologies. The more the aspirational consumers want to drive such cars, the more the slithering power of Tesla and other similar companies grows, including their harmful effects.

Bibliography

ACLU. 2014. War comes home. The excessive militarization of American policing. https://www.aclu.org/report/war-comes-home-excessive-militarization-american-police [accessed April 4, 2021].

Ahmad, S., & Khan, M. (2019). Tesla: Disruptor or sustaining innovator. *Journal of Case Research, 10*(1), 12–24.

AutoBlog. (2021). Tesla update activates the in-car camera for driver monitoring. https://www.autoblog.com/2021/05/30/tesla-in-car-camera-driver-monitoring/ [accessed June 18, 2021].

Auto Connected Car. (2014). Definition of connected car – What is the connected car? Defined. https://www.autoconnectedcar.com/definition-of-connected-car-what-is-the-connected-car-defined/ [accessed April 23, 2021].

AutoExpress. (2020). Tesla Model S review – Engines, performance and drive. https://www.autoexpress.co.uk/tesla/model-s/engines [accessed June 18, 2021].

Axsen, J., Cairns, J., Dusyk, N., & Goldberg, S. (2018). What drives the pioneers? Applying lifestyle theory to early electric vehicle buyers in Canada. *Energy Research & Social Science, 44*, 17–30.

Barry, K. (2021). Tesla's in-car cameras raise privacy concerns. https://www.consumerreports.org/privacy/teslas-in-car-cameras-raise-privacy-concerns/ [accessed April 3, 2021].

Bauman, Z. (1999). Modernity as history of time. *Concepts and Transformation, 4*(3), 229–248.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation.* Polity.

Bayley, D., & Shearing, C. (1996). The future of policing. *Law and Society Review, 30*(3), 585–606.

BBC. (2021). Tesla: Elon Musk suggests autopilot not to blame for fatal crash. https://www.bbc.com/news/technology-56799749 [accessed June 5, 2021].

Beck, U. (1992). *Risk society: Towards a new modernity.* Sage.

Beene, R. (2018) Tesla accused of deception in promoting autopilot technology. https://www.bloomberg.com/news/articles/2018-05-23/tesla-s-autopilot-promotions-are-deceptive-watchdog-groups-say [accessed March 8, 2022].

Bellanova, R., K. Irion, K. Lindskov Jacobsen, F. Ragazzi, R. Saugmann & L. Suchman (2021). Toward a critique of algorithmic violence. *International Political Sociology, 15*(1), 121–150.

Bolca, T. (2019). Big Brother Riding Shotgun: Internal Surveillance of Semi-Autonomous Vehicles and its Effects on the Reasonable Expectation of Privacy. *Canadian Journal of Law and Technology, 17*(1): 77–89.

Buckey, A.W. (2019). Surveillance. ABDO.

Canellas, M., & Haga, R. (2020). Unsafe at any level. *Communications of the ACM, 63*(3), 31–34.

Cantu, M. (2021). Check Out How Tesla's In-Cabin Camera Analyses Your Face. https://insideevs.com/news/499611/tesla-cabin-camera-analyses-you/ [accessed April 29, 2021].

Chen, A. (2018). Elon Musk wants cobalt out of his batteries — here's why that's a challenge. https://www.theverge.com/2018/6/21/17488626/elon-musk-cobalt-electric-vehicle-battery-science [accessed June 1, 2021].

Cooke, P. (2021). Three Disruptive Models of New Spatial Planning: "Attention", "Surveillance" or "Sustainable" Capitalisms? *Journal of Open Innovation: Technology, Market, and Complexity, 7*(46), 1–20.

Coulthard, D. & Keller, S. (2010). A social ecological model of ICT cooption: Surveillance creep in the information age. *ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems.* ACIS.

Cowan, R. S. (1983). *More Work for Mother: The Ironies of Household Technology From the Open Hearth to the Microwave.* Basic Books.

Crawford, K. (2021). *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence.*

Yale University Press.
Crothers, B. (2015). Tesla Executive Pushes Back At Critics Characterizing It As Elitist: Report. https://www.forbes.com/sites/brookecrothers/2015/08/05/tesla-executive-pushes-back-at-critics-characterizing-it-as-elitist-report/ [accessed March 8, 2022].
Currid-Halkett, E. (2017). *The sum of small things: A theory of the aspirational class.* Princeton University Press.
Dandeker, C. (2006). Surveillance and military transformation: Organizational trends in twenty-first century armed services. In K. Haggerty & R. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 225–249). University of Toronto Press.
Deka, K. (2021). Of imported SUVs and buying "The Last Supper" in Milan: "New middle class" and its crisis of hegemony in India's Northeast. In M.K. Jha & Pushpendra (eds.) B*eyond consumption. India's New Middle Class in the Neo-Liberal Times* (pp. 154–170). Routledge.
Denman, D. (2020). The logistics of police power: Armored vehicles, colonial boomerangs, and strategies of circulation. *EPD: Society and Space, 38*(6), 1138–1156.
Dong, Y., Hu, Z., Uchimura, K., & Murayama, N. (2010). Driver inattention monitoring system for intelligent vehicles: A review. *IEEE transactions on intelligent transportation systems, 12*(2), 596–614.
Edenius, M. (2006). The Function of Representation in a "Smart Home Context". *International Journal of Technology and Human Interaction, 2*(3), 1–15.
EDPB. (2020). Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf [accessed May 18, 2021].
Eikenberry, A. M., & R. Mirabella (2018). Extreme philanthropy: Philanthrocapitalism, effective altruism, and the discourse of neoliberalism. *Political Science and Politics, 51*(1), 43–47.
Electrive (2020). Tesla in taxi trouble in Holland. https://www.electrive.com/2020/12/09/tesla-in-taxi-trouble-in-holland/ [accessed May 3, 2021].
Ericson, R.V. & K.D. Haggerty (1997). *Policing the risk society.* University of Toronto Pres Inc.
EVANNEX (2020). Tesla Wins PC Magazine's Readers' Choice Award for Connected Cars https://insideevs.com/news/432348/tesla-connected-car-award-pc-magazine-readers/ [accessed June 11, 2021].
Feeley, M., & J. Simon (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology, 30*(4), 449–474.
Feldstein, S. (2019). *The global expansion of AI surveillance.* Carnegie Endowment for International Peace.
Fortuna, C. (2019). What do we know about Tesla owners? https://cleantechnica.com/2019/06/01/what-do-we-know-about-tesla-owners/ [accessed May 3, 2021].
Foucault, M. (2003). *Society Must Be Defended: Lectures at the Collège de France, 1975–76.* Picador.
Fridson, M. S. (1999). *How to be a Billionaire: Proven Strategies from the Titans of Wealth.* John Wiley and Sons.
Garfunkel, D. (2021). Between ownership and privacy: Private surveillance and condominium governance in Israel. In Lippert, R. K., & Treffers, S. (eds.) *Condominium Governance and Law in Global Urban Context* (pp. 82–97). Routledge.
Gasgoo (2020). Tesla recalls imported Model Ss, Model Xs in China. http://autonews.gasgoo.com/new_energy/70017665.html [accessed May 3, 2021].
Gilchrist, A. (2017). The Panopticon. *In IoT security issues* (pp. 229–256). De| G Press.
Gilliard, C., & D. Golombia (2021). Luxury surveillance. https://reallifemag.com/luxury-surveillance/ [accessed August 3, 2021].
Gordon, C. (2019). *Citizen Brown: Race, Democracy, and Inequality in the St. Louis Suburbs.* University of Chicago Press.
Graham, S. (2011). *Cities Under Siege: The New Military Urbanism.* Verso.

Gregory, D. (2004). The Colonial Present. Blackwell.

Halliday, J. (2013). Top Gear Row: Tesla loses appeal over Jeremy Clarkson review. https://www.theguardian.com/media/2013/mar/05/top-gear-tesla-jeremy-clarkson [accessed June 18, 2021].

Hess, D. J. (2020). Incumbent-led transitions and civil society: Autonomous vehicle policy and consumer organizations in the United States. Technological Forecasting and Social Change, 151, 119825.

Hijink, M. (2021). Opletten! Je auto houdt je in de gaten. https://www.nrc.nl/nieuws/2021/04/02/opletten-je-auto-houdt-je-in-de-gaten-a4038356 [accessed June 18, 2021].

HLDI (2018). Insurance report. Noncrash fire losses. https://www.iihs.org/media/c93b98d8-6a7d-44a1-810e-4468ec539e05/uIu4tg/HLDI%20Research/Fire%20losses/HLDI_Fire-Losses_1218.pdf [accessed March 8, 2022].

Honningsvåg, C. (2019). Skadestatistikk: Elbiler bulker mest. https://www.elbil24.no/nyheter/elbiler-bulker-mest/71498210 [accessed March 8, 2022].

Ingeborgrud, L. & M. Ryghaug (2017). User perceptions of EVs and the role of EVs in the transition to low-carbon mobility. *ECEEE Summer Study Proceedings,* 893-900.

Ingle, S. and M. Phute (2016). Tesla autopilot: semi-autonomous driving, an uptick for future autonomy. *International Research Journal of Engineering and Technology, 3*(9), 369-372.

Jamil, R. (2020). Uber and the making of an Algopticon-Insights from the daily life of Montreal drivers. *Capital & Class, 44*(2), 241-260.

Johnston, L. and C. Shearing (2003). *Governing Security: Explorations in Policing and Justice.* London: Routledge.

Jonsson, K. (2006). The embedded panopticon: visibility issues of remote diagnostics surveillance. *Scandinavian journal of information systems, 18*(2), 3.

Kester, J., de Rubens, G. Z., Sovacool, B. K., and Noel, L. (2019). Public perceptions of electric vehicles and vehicle-to-grid (V2G): Insights from a Nordic focus group study. *Transportation Research Part D: Transport and Environment, 74*, 277-293.

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences.* London: Sage.

Lambert, F. (2017). Tesla's new steering wheel comes with Autopilot sensor-based drive modes, force touch buttons, and more. https://electrek.co/2021/01/27/tesla-new-steering-wheel-force-touch-buttons-autopilot-sensors/ [accessed May 18, 2021].

Lambert, F. (2018). Tesla hires machine learning experts as new VP of Engineering working on Autopilot – among other things. https://electrek.co/2018/05/22/tesla-hires-machine-learning-expert-new-vp-of-engineerin-autopilot/ (accessed March 11, 2022].

Lambert, F. (2021). Tesla starts suing former customers for defamation in China. https://electrek.co/2021/09/30/tesla-starts-suing-former-customers-defamation-in-china/ [accessed March 8, 2022].

Levin, T. (2022). A Tesla car came to a complete stop on an interstate, police say, causing a 3-car crash that killed the driver. https://www.businessinsider.com/tesla-crash-driver-killed-after-car-stops-on-highway-2022-3?international=true&r=US&IR=T [accessed March 8, 2022].

Levine, J. and J. Simpson (2018). Request for Investigation of Deceptive and Unfair Practices in Advertising and Marketing of the "Autopilot" Feature Offered in Tesla Motor Vehicles. https://www.autosafety.org/wp-content/uploads/2018/05/CAS-and-CW-Letter-to-FTC-on-Tesla-Deceptive-Advertising.pdf [accessed May 3, 2021].

Liebenberg, I. (2015). Penetrating global consciousness: Art, killing as art, art as subversion, peace and the inversion of speed and power. *Cogent Arts and Humanities, 2*(1), 1-22.

Loader, I. (2000). Plural policing and democratic governance. *Social and legal studies, 9*(3), 323–345.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination.* New York:

Routledge.
Lyytinen, K. and Y. Yoo (2002). Issues and challenges in ubiquitous computing. *Communications of the ACM, 45*(12), 63-65.
Maalsen, S. and J. Sadowski (2019). The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance. *Surveilance and Society, 17*(1/2), 118–124.
Macri, K.P. (2018). Case study: How Tesla changed the auto industry. https://www.supplychaindive.com/news/case-study-how-tesla-changed-the-auto-industry/517251/ [accessed March 3, 2022]
Magalhães, J.C. and N. Couldry (2021). Giving by taking away: Big tech, data colonialism, and the reconfiguration of social good. *International Journal of Communication, 15*, 343–362.
Marx, G. (2016). *Windows into the Soul, Surveillance and society in an age of high technology.* Chicago: University of Chicago Press.
McAfee, A. and E. Brynjolfsson (2017). M*achine, platform, crowd: Harnessing our digital future.* London: WW Norton and Company.
Mills, A. and M. Mills (2014). The Invention of the War Machine. *The New Atlantis, 42*, 3-23.
Moran, R.E. (2020). Examining switching power: Mark Zuckerberg as a novel networked media mogul. *Information, Communication and Society, 23*(4), 491-506.
Moskowitz, C. (2012). SpaceX Launches Private Capsule on Historic Trip to Space Station. https://www.space.com/15805-spacex-private-capsule-launches-space-station.html [accessed November 4, 2021].
Murtola, A-M. (2018). How the global tech elite imagine the future. *Economic and Social Research Aotearoa, 11*, 1–12.
Naafs, S. and P. Weijnen (2020). U rijdt zo langs ons Big Mac-menu. https://www.groene.nl/artikel/u-rijdt-zo-langs-ons-big-mac-menu [accessed May 18, 2021].
Nygaard, B. (2019). Driving Towards a Greener Future: A qualitative study of Tesla owners' green practices in a Danish Context. https://lup.lub.lu.se/student-papers/search/publication/8983907 [accessed June 11, 2021].
Packer, J. (2006). Becoming bombs: Mobilizing mobility in the war of terror, *Cultural Studies, 20*:4-5, 378-399.
Pali, B. & M. Schuilenburg (2020). Fear and Fantasy in the Smart City, *Critical Criminology: An International Journal, (28)*4, 775-788.
Park, K.M. (2020). The New Executive: Interconnected Yet Isolated and Uninformed–Leadership Challenges in the Digital Pandemic Epoch. In *The Palgrave Handbook of Management History,* B. Bowden et al. (eds.), pp. 1011–1045. London: Palgrave Macmillan.
Perzanowski, A. and J. Schultz (2016). *The end of ownership: Personal property in the digital economy.* Boston: MIT Press.
Polson, E. (2019). The Aspirational Class "Mobility" of Digital Nomads. In *The Routledge Companion to Media and Class*, E. Polson, L. Schofield Clark, R. Gajjala (eds.), pp. 168-179. London and New York: Routledge.
Pridmore, J. (2012). Consumer surveillance: Context, perspectives and concerns in the personal information economy. In *Routledge Handbook of Surveillance Studies*, K. Ball, K.D. Haggerty and D. Lyon (eds.), pp. 321-329. London and New York: Routledge.
PR Newswire (2014). Tesla Provides Best Connected Vehicle User Experience says Strategy Analytics. Retrieved from: https://www.prnewswire.com/news-releases/tesla-provides-best-connected-vehicle-user-experience-says-strategy-analytics-259408551.html [accessed June 3, 2021].
Ribeiro, H. and L. Tang (2020). EV makers' battery choices raise questions about future cobalt demand. https://www.spglobal.com/platts/en/market-insights/blogs/metals/111120-ev-batteries-cobalt-demand-tesla-volkswagen-byd-bmw [accessed May 27, 2021].
Rosenblat, A., T. Kneese and D. Boyd (2014). Workplace surveillance. O*pen Society Foundations' Fu-*

ture of Work Commissioned Research Papers.

Sadowski, J. & R. Bendor (2018). Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary. *Science, Technology & Human Values, 44*(3), 540-563.

Sadowski, J., Y. Strengers and J. Kennedy (2021). More work for Big Mother: Revaluing care and control in smart homes. Environment and Planning A: Economy and Space. https://doi-org.vu-nl.idm.oclc.org/10.1177/0308518X211022366 [accessed May 2, 2021].

Safransky, S. (2020). Geographies of algorithmic violence: Redlining the smart city. *International Journal of Urban and Regional Research, 44*(2), 200-218.

Sakamoto, K. (2014). How Tesla Plans to Lead the Connected Car Experience. Retrieved from: https://www.carthrottle.com/post/how-tesla-plans-to-lead-the-connected-car-experience/ [accessed May 18, 2021].

Schmidt, A. et al. (2021). *What sustainable drivers want. Busting the myths of sustainability: A wake-up call for automakers.* Accenture: Stuttgart.

Schmidt, B. (2020). Tesla Cybertruck may be unsafe for other road users, says Australian safety chief. The Driven. https://thedriven.io/2019/11/27/tesla-cybertruck-may-be-unsafe-for-other-road-users-says-australian-safety-chief/#:~:text=Chief%20executive%20of%20Australian%20car,road%20users%20such%20as%20pedestrians. [accessed March 8, 2022].

Schuilenburg, M. (2015). *The Securitization of Society. Crime, Risk, and Social Order.* New York: NYU-Press.

Shepardson, D. (2020). U.S. agency opens probe into 115,000 Tesla vehicles over suspension issue. https://www.reuters.com/article/us-tesla-safety-investigation/u-s-agency-opens-probe-into-115000-tesla-vehicles-over-suspension-issue-idUSKBN287172 [accessed April 11, 2021].

Smith, M.R.H. et al. (2008). A Final Report of Safety Vehicles using adaptive Interface Technology (Phase II: Task 9C): Adaptive Safety Warning Countermeasures. https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/SAVE-IT%20-%20Adaptive%20Safety%20Warning%20Countermeasures.doc [accessed May 18, 2021].

Solomon, L.D. (2011). *Tech Billionaires: Reshaping Philanthropy in a Quest for a Better World.* London: Transaction.

Sørensen, K.H., & J. Sørgaard (1994). Mobility and modernity: towards a sociology of cars. *The Car and Its Environments, Brussels: ECSC-EECEAEC.*

Sovacool, B. K., Kester, J., Noel, L., and de Rubens, G. Z. (2019). Energy injustice and Nordic electric mobility: Inequality, elitism, and externalities in the electrification of vehicle-to-grid (V2G) transport. *Ecological economics, 157*, 205-217.

Srnicek, N. (2016). *Platform capitalism.* Cambridge: Polity.

Staver, J. (2021). Tesla Autopilot Fatality Rate. https://www.chicagolawyer.com/blog/tesla-autopilot-fatality-rate/ [accessed March 8, 2022].

Stelling-Kończak, A., M. Hagenzieker and B. Van Wee (2015). Traffic sounds and cycling safety: The use of electronic devices by cyclists and the quietness of hybrid and electric cars. *Transport Reviews, 35*(4), 422-444.

Stillerman, K. (2020). Tesla Owner Demographics: Age, Gender, Ethnicity, Income, Children. https://www.evunite.com/blog/tesla-owner-demographics/ [accessed June 10, 2021].

Taffel, S. (2018). Hopeful Extinctions? Tesla, Technological Solutionism and the Anthropocene. *Culture Unbound, 10*(2): 163–184.

Tangermann, V. (2019). A Tesla driver was eating, drinking during autopilot crash. https://futurism.com/the-byte/tesla-driver-eating-drinking-autopilot-crash [accessed May 18, 2021].

Teece, D. (2018). Tesla and the reshaping of the auto industry. *Management and Organization Review, 14*(3), 501-512.

Templeton, B. (2020). Teslas aren't safer on autopilot, so researchers calling for driver mon-

itoring may be right. https://www.forbes.com/sites/bradtempleton/2020/07/28/teslas-arent-safer-on-autopilot-so-researchers-calling-for-driver-monitoring-may-be-right/?sh=5c5d371b1d73 [accessed March 8, 2022].

Tesla (2020). Tesla comments on EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/tesla_comments_edpb_guidelines_30apr2020_0_0.pdf [accessed May 18, 2021].

Tesla (2021a). Car Safety and Security Features. https://www.tesla.com/support/car-safety-security-features?redirect=no [accessed June 3, 2021].

Tesla (2021b). Support – Software updates. https://www.tesla.com/support/software-updates?redirect=no [accessed June 3, 2021].

Tesla (2021c). Support – Discover Software Version 10.0. https://www.tesla.com/support/software-version-10-0 [accessed June 3, 2021].

Tesla (2021d). The Mission of Tesla. https://www.tesla.com/nl_NL/blog/mission-tesla?redirect=-no [accessed May 11, 2021].

Tillman, M. (2021). Tesla models compared: Model S, Model 3, Model X, Model Y, Cybertruck and more. https://www.pocket-lint.com/cars/news/tesla/137055-tesla-everything-you-need-to-know [accessed May 11, 2021].

Timmer, J. (1998). Chroom en charisma een sociologisch essay over de auto. *Mens & Maatschappij, 73*(2), 157–175.

Torchinsky, J. (2018). Consumer Group Says Tesla's Autopilot Is 'Deceptive,' Calls for Investigation. https://jalopnik.com/consumer-group-says-teslas-autopilot-is-deceptive-call-1826249830 [accessed April 11, 2021].

Tusikov, N. (2019a). Defunding hate: PayPal's regulation of hate groups. *Surveillance & Society, 17*(1/2), 46-53.

Tusikov, N. (2019b). Regulation through "bricking": private ordering in the "Internet of Things". *Internet Policy Review, 8*(2), 1-18.

Vance, A. (2015). *Elon Musk: How the billionaire CEO of SpaceX and Tesla is shaping our future.* London: Virgin.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society, 12*(2), 197-208.

Virilio, P. (1994). *Bunker Archeology.* New York: Princeton Architecture Press.

Virilio, P. (2006). *Speed and Politics.* Los Angeles: Semiotext(e).

Weiser, M. (1991). The computer for the 21st century. Scientific American September: 66-75.

Weiss, N., M. Schreieck, M. Wiesche and H. Krcmar (2020). From Product to Platform: How can BMW compete with Platform Giants? Journal of Information Technology Teaching Cases. Online first: 1–11.

Wilson, D. (2012). Military Surveillance. In *Routledge Handbook of Surveillance Studies*, K. Ball, K.D. Haggerty and D. Lyon (eds.), (pp. 269-276). London and New York: Routledge.

Wright, P. (2001). *Tank: The Progress of a Monstrous War Machine.* London: Faber and Faber.

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.

Yarin Eski, is an assistant professor in Public Administration at the Knowledge Hub Security and Social Resilience of the VU Amsterdam. His research and teaching cover the themes of (maritime) security, ethnography, policing, biography, the arms trade, illegal drug trafficking, corruption, genocide. His work includes A Criminological Biography of an Arms Dealer (2022), Genocide & Victimology (Routledge, 2020), and Policing, Port Security and Crime Control (Routledge, 2016). Moreover, he is a Fellow of the Higher Education Academy in the United Kingdom and obtained his PhD in 2015 from the University of Glasgow. He is an associate member of the Strategic Hub for Organised Crime Research (SHOC) of the Royal United Services Institute (RUSI) and of the Scottish Centre for Crime and Justice Research (SCCJR).

Marc Schuilenburg,is Professor of Digital Surveillance at Erasmus University Rotterdam and Assistant-Professor Criminology at VU Amsterdam. He has published the critically and highly acclaimed books Hysteria (Routledge, 2021), The Securitization of Society (NYU-Press, 2015) and Mediapolis (010-Publishers, 2006). He has edited eight books, including The Algorithmic Society (Routledge, 2021). His PhD on security assemblages in urban environments was awarded the triennial Willem Nagel Prize by the Dutch Society of Criminology. He has been a visiting professor in New York (John Jay College, 2013) and Ipswich (University Campus Suffolk, 2014-2020). Internet: www.marcschuilenburg.nl.

How to cite this article (APA– 7th ed.): Eski, Y., & Schuilenburg, M. (2022). On Tesla: Balancing sustainable car connectivity, silent lethality and luxury surveillance. *Criminological Encounters*, *5*(1), 234-251. https://doi.org/10.26395/CE22050118