

# Counter-Mapping the Spaces of Autonomous Driving

Luis F. Alvarez León  
Dartmouth College  
luis.f.alvarez.leon@dartmouth.edu

*In this article I provide an account of key tensions shaping the development of autonomous driving technologies, and explore how such tensions can open up avenues for counter-mapping the data spaces produced through these navigation technologies. The design and massive commercialization of autonomous vehicles implies the production of new models of space, generated through the integration of data collected through technologies such as lidar scanning, machine learning, and artificial intelligence. This production of space is bounded within the confines of the technological black boxes of the vehicles themselves, as well as the corporate black boxes of the companies that design and deploy them. However, there are key sources of tension surrounding the creation of these black boxes: those between market competitors; between the state and the private sector; and between civil society, the private sector, and the state. In this article I explore these tensions by focusing on the potential for counter-mapping as a means of critique, transparency, and political action across three separate aspects of the autonomous driving space-making process: (1) legislation, by examining the emergence of Right to Repair laws across the United States, beginning with the Automotive Right to Repair Law passed in Massachusetts in 2012; (2) design, through open source projects for building self-driving cars, exemplified by Udacity, a pioneer in this area; and (3) hacking, specifically interventions designed to open, critique, or disrupt autonomous driving technologies. These examinations are embedded in a political economic account that interrogates the ownership and control over the spaces produced through autonomous driving, as well as the economic value associated with such production of space.*

**KEYWORDS:** counter-mapping; autonomous driving; automated mapping; Right to Repair; hacking; artificial intelligence; machine learning; open-source design

## INTRODUCTION

OVER THE PAST FIVE YEARS, autonomous vehicles have gone from one of many in an expanding constellation of innovations to the touchstone technology upon which a particular vision of the future is articulated. Autonomous vehicles represent a significant step in the integration of the digital information economy with the automobile industry (Gao, Hensley, and Zielke 2014; Lipson and Kurman 2016)—perhaps the archetypal industry of twentieth-century capitalism. While there is some evidence that younger cohorts prefer ride-sharing as a means of transportation—which could in principle be satisfied by self-driving cars—(Krueger, Rashidi, and Rose 2016), there are fundamental questions about how (by, and for whom) this technology would be deployed. For all the potential benefits of autonomous vehicles, the corporate push favoring them over existing modes of public transportation exceeds any current demand, while simultaneously advancing an emerging

digital urban capitalism that is predicated on the rhetoric of “smart” or “data-driven” cities and the intensified privatization of services (Cugurullo 2018; Shelton, Zook, and Wiig 2015; Wiig 2018). At the heart of autonomous navigation is the production of new cartographies that allow automated vehicles to be deployed through physical spaces—and, in the process, influence economic processes as well as the organization of urban systems and transportation infrastructure (Schlossberg et al. 2018). These maps are created through sophisticated, and often proprietary, combinations of sensing and mapping technologies, which feature continuous, multimodal, and extensive data collection and processing. Thus, in navigating, and potentially transforming, space, autonomous vehicles effectively produce new virtual spaces through processes enclosed within technological as well as corporate black boxes. In combining pre-existing digital maps with continuously updated



© by the author(s). This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0>.

spatial databases that respond to the vehicles' navigation of space, the maps at the core of autonomous driving enact both the representational and performative possibilities of cartography: they are both object and process.

Given the magnitude of the resources invested in autonomous vehicles, their expected knock-on effects,<sup>1</sup> and their potential to reshape cities and socioeconomic organization, the mechanisms underlying their navigation of space should be more open to public scrutiny, deliberation, and regulation. My goal in this article is to expand the emerging conversation on the politics of autonomous vehicles (Bissell 2018; Boeglin 2015; Brodsky 2016; Stilgoe 2018) by advancing counter-mapping as a means to open up the spaces produced by, and for, autonomous driving. I will examine three separate possible avenues for counter-mapping: (1) *legislation*, specifically the emergence of right-to-repair laws across the United States, beginning with the Automotive Right to Repair Law passed in Massachusetts in 2012; (2) *design*, through open source projects for building self-driving cars, exemplified by Udacity, a pioneer in this area; and (3) *hacking*, specifically interventions proposed or designed to open, critique, or disrupt autonomous driving technologies.

I have identified these three aspects because they exemplify significant nodes of interaction between various actors in society, such as the public, interest groups, and legislators (legislation); firms, advocate groups, and consumers (design); and counter-cultural groups, regulators, information security advocates, and the media (hacking). After exploring these avenues, I will embed them in a political economic account that interrogates the ownership and control over the spaces produced through autonomous driving, as well as the data-harvesting and economic value generation associated with such production of space.

## COUNTER-MAPPING

In her foundational contribution describing the struggles over forest resources in Kalimantan, Indonesia, Nancy Peluso (1995, 384) characterizes counter-mapping as a strategy used by local activists and allies to “appropriate the state’s *techniques* and *manner of representation* to bolster the legitimacy of ‘customary’ claims to resources.” Harris and Hazen, in turn, provide a more extensive conception

of counter-mapping that incorporates “any effort that fundamentally questions the assumptions or biases of cartographic conventions, that challenges predominant power effects of mapping, or that engages with mapping in ways that upset power relations” (2005, 115). As suggested by these definitions, counter-mapping exists and evolves through a symbiotic relationship with established, accepted, and conventional technologies of mapping and modes of spatial representation, construction, and performance.

Over the past two decades, counter-mapping has closely tracked new developments in geospatial data, media, and technologies with the aim of turning them on their head and critically interrogating their established uses. Counter-mapping has been used by students and activists speaking against university policies (Counter Cartographies Collective, Dalton, and Mason-Deese 2012), indigenous peoples staking claims to land and resources (Wainwright and Bryan 2009), critics challenging architectural orthodoxies (Cattoor and Perkins 2014), researchers seeking to make conservation more equitable and effective (Harris and Hazen 2005), migrant advocates identifying routes into Europe (Casas-Cortés et al. 2017), activists reclaiming queer spaces and lived experiences in the city (Gieseck 2016), and scholars exposing privacy violations and passive data collection (Propen 2005). As these wide-ranging examples demonstrate, counter-mapping is less defined by any one technology, method, or mode of spatial representation, and more by an ethos of challenging power asymmetries in (and through) the mapping and appropriation of space.

Today’s informational environment is increasingly characterized by the ascendance of technologies that bring order-of-magnitude increases in the speed, volume, and sophistication of data collection and processing (Kitchin 2014; Mayer-Schönberger and Cukier 2013). Three well publicized, trendsetting examples are social computing, blockchain, and artificial intelligence. While these and other influential technologies can be identified by their technical specifications and capabilities, they should also be understood through their linkages with and functional integration into the dynamics of digital capitalism. In this context, counter-mapping has a crucial role to play—mobilized through a variety of new tools and approaches that reflect the very technologies used to exert power through mapping.

1. A study commissioned by processor maker Intel, and conducted by the firm Strategy Analytics in 2017, estimates that the widespread adoption of fully automated vehicles will catalyze a new global passenger economy worth \$7 trillion USD by 2050 (Lancot 2018).

Counter-mapping can be a productive approach in checking and contesting new technical and political-economic regimes because its range and generative potential transcends the realm of spatial products (and processes) narrowly defined as “maps.” As a way of thinking, acting, and producing spatial and political knowledge from a critical standpoint, counter-mapping not only deals with spatial objects that are immediately visible; it can also help excavate them from places that are hidden from plain view, or re-enact them through different perspectives. One example of this is the realm of “big data” and its emerging disciplinary counterpart, “data science.” By counter-mapping “data science” itself, Dalton and Stallman (2017) elucidate the spatial relations involved in, and produced by, established modes of data production and interpretation—which are often in the service of powerful actors, such as corporations, states, and academic elites. In order to challenge the power-inflected spatial representations found in big data and data science, we can mobilize counter-mapping to connect theory and practice, and re-situate it in a bottom-up perspective:

Counter-mapping offers both theorists and practitioners a way to connect careful, situated approaches to data . . . to the enacted practices of social organizing and change-making. It can combine critical thought and practice to draw on data science sources and methods (often developed by or for large corporations), yet does so in a situated, bottom-up manner to realize different ends. (Dalton and Stallmann 2017, 3)

Along similar lines, Shannon Mattern (2017) has argued for the need to question and challenge the new spatialities intertwined with emerging technologies of navigation and automated transportation. The growth of automated vehicles—as an industry, as a transportation paradigm, and as an ideology of mobility—has been fully embraced by the Silicon Valley elite (as well as counterparts in China and other countries) and is already transforming the global automobile industry. In the same way that medieval towns bear the imprint of horse-drawn carriages, and twentieth-century cities were (re)organized to accommodate (and often privilege) cars, it seems increasingly likely that the urban forms of the twenty-first century will be deeply influenced by the expansion of automated vehicles. In light of this world in emergence, it is imperative to ask, as Mattern does,

. . . critical questions about how machines conceptualize and operationalize space. How do they render our world measurable, navigable, usable, conservable? We must also ask how those artificial intelligences, with their digital sensors and deep learning models, intersect with cartographic intelligences and subjectivities beyond the computational “Other.” . . . There are a lot of *other* Others—including marginalized and indigenous populations and non-human environmental actors—who belong on the map, too, and not merely as cartographic subjects. They are active mapping agents with distinct spatial intelligences, and they have stakes in the environments we all share. (Mattern 2017)

Asking such questions requires prying open the black boxes that contain new mappings underlying automated vehicles. This is not only a technical exercise, but also a political act, since such black boxes are the means by which new modes of spatial representation, navigation, and performance (and, by extension, new articulations of power in space) remain hidden from public deliberation. Inflected by power and capital as they are, these mappings embody the asymmetries at the core of digital capitalism: while they use public spaces, personal information, and common-pool resources as inputs to generate economic value, they remain closed to deliberation or input from those who will bear the consequences of their deployment.

Accordingly, actions such as examining, disrupting, repairing, distributing, or reproducing the mechanisms and information underlying autonomous navigation often constitute infringements due to their proprietary nature, and legislation that reinforces it. These restrictions are part and parcel of a growing economy of information and digital technologies fueled by data collection, and dependent upon closed ecosystems as a way of ensuring profits.

Counter-mapping, as an ethos that can be put in practice through myriad techniques, actions, and perspectives, offers a promising opportunity to take apart the spaces produced within the black boxes of autonomous vehicles and the corporations that own them, in order to reconstruct them for other means. A provocative potential outcome, suggested by Manaugh (2016), is to make use of spaces of misdirection that, instead of making a robot-readable

world, create one that is illegible to them. While the precise nature of the world we build should be the product of collective deliberation and participatory decision-making, a necessary step is to reclaim agency from the technical and economic assemblages (such as autonomous vehicles) that are currently redrawing the very spaces where we circulate and inhabit. The mapping conducted by autonomous vehicles follows two general approaches, each of which relies on particular technological configurations, and carries with it potentially different space-making consequences:

One aims to create complete high-definition maps that will let the driverless cars of the future navigate all on their own; another creates maps piece-by-piece, using sensors in today's vehicles that will allow cars to gradually automate more and more parts of driving. (Bergen 2018)

Each of these approaches captures the world in a particular way, representing and recreating it in a manner that is suitable for a specific array of navigational technologies—often backed by a collection of corporate interests and alliances betting on the “winning” combination (Bergen 2018; Evans 2017; Hook and Bott 2018). Once captured, this three-dimensional re-creation of the world then becomes the setting for action of the vehicle itself, as well as those who make decisions about its navigation (including the human passengers who input directions, the engineers

who design how the car will determine its path, and the advertisers analyzing new data streams for optimal placements along the way). However, the potential for action embedded in these mappings transcends the immediate navigational needs of the vehicle, since they can be used for decision making in other realms, such as managing traffic patterns, conducting street repairs, surveillance, marketing, urban planning, and even infrastructural upgrades. Yet, these activities are tied to, and would depend directly on, the type, quality, and characteristics of the spatial information collected and presented by the navigational technologies that produce such mappings—all of which are secretly guarded within technological and corporate black boxes.

In this article, I propose three specific avenues through which counter-mapping can be mobilized to open the black boxes of autonomous driving for deliberation, contestation, and transformation. In the next section I show how legislation, design, and hacking can challenge the technical, legal, and corporate barriers that guard the production of spaces at the core of autonomous driving. In the subsequent section, I integrate insights from these avenues into a political economic account centered on the ownership and control of spaces in the context of automated vehicles, and the generative potential (along with potential ramifications) of counter-mapping to facilitate alternative orders. The final section suggests future directions of inquiry and political intervention.

## AVENUES FOR COUNTER-MAPPING

### LEGISLATION

STARTING IN THE 1990S, auto manufacturers positioned themselves as gatekeepers of the information required to repair (increasingly computerized) car systems, as well as who is authorized to do so. A practical consequence of this has been the funneling of repair work to manufacturer-authorized car dealerships, to the disadvantage of independent mechanics and auto repair shops (Kessler 2017). As cars become digitally networked to auto manufacturers, other cars, or even infrastructure, the issue of access to car data by third-party repair services will become a more salient point of contention both for mechanics and for consumers. However, these discussions can also inform debates on broader issues about ownership and access to any

sort of digital information collected by, and stored within automobiles. In light of the ongoing computerization and networking of cars, repair data constitute a useful (legal and conceptual) precedent for the expanding data ecosystems of automated vehicles.

The high barriers and costs to repair automobiles have galvanized grassroots movements that aim to broaden access to repair capabilities. Cars have become a focal point in the emerging Right to Repair movement due to their intensified computerization, the growing momentum of automated vehicles, and the size of the aftermarket for third-party repair services. As one mechanic put it, the

survival of the trade is contingent on “fair and equal access to data, information, and training” (Kessler 2017). Furthermore, calls for the right to repair are symptomatic of broader contestations challenging restrictive notions of ownership and closed access that have come to define digital capitalism (Perzanowski and Schultz 2016). Thus, organizations representing users of smartphones, computers, printer cartridges, and other electronics—such as the Electronic Frontier Foundation ([eff.org/issues/right-to-repair](http://eff.org/issues/right-to-repair)), the Institute of Electrical and Electronics Engineers ([spectrum.ieee.org/green-tech/conservation/why-we-must-fight-for-the-right-to-repair-our-electronics](http://spectrum.ieee.org/green-tech/conservation/why-we-must-fight-for-the-right-to-repair-our-electronics)), and iFixit ([ifixit.org/right](http://ifixit.org/right))—have expressed their discontent with what they see as restrictive (and wasteful) practices by the corporations that seek to control, not only the manufacture and distribution, but also the use, transformation, and resale of products.

These informational enclosures have catalyzed a legislative movement in the United States aimed at making repair information available to consumers as well as independent shops. At the federal level, the first Right to Repair bill was introduced in 2001, but was not adopted. In 2013, after reconciling two separate laws enacted the previous year, Massachusetts passed the first Right to Repair legislation (An Act Relative to Automotive Repair 2013). In 2017, the state’s Consumer Protection and Professional Licensure Committee heard legislation that would expand the Right to Repair to cover all types of electronics sold in the state. As it continues to be considered by the legislature, this expansion is actively opposed by manufacturers in the appliance, video game, electronics, and medical device industries, along with others that have a financial stake in maintaining control of the repair services market (Metzger 2017).

The original Massachusetts Right to Repair legislation led to a Memorandum of Understanding between automakers (represented by the Alliance of Automobile Manufacturers and the Association of Global Automakers) and third-party service providers (represented by the Automotive Aftermarket Industry Association, and the Coalition for Auto Repair Equality), in which the former committed to provide the necessary information for repairs to the latter, beginning with 2018 car models across all 50 U.S. states (Bassett 2016). However, while at the time of this writing eighteen states<sup>2</sup> have introduced legislation on the

Right to Repair electronics and other devices ([www.theverge.com/2018/3/8/17097256/california-right-to-repair-bill-apple-microsoft-service-replace-parts](http://www.theverge.com/2018/3/8/17097256/california-right-to-repair-bill-apple-microsoft-service-replace-parts)), it remains unclear how the Right to Repair movement and ensuing legislation will inform the governance of data collected by automated vehicles once their use is more widespread. An important point to consider is the changing nature of technology, and its slippery relationship with legislation, which is often less dynamic. In the case of automobiles, the 2014 agreement to share car data with repair shops represents a step in the direction of a more open informational environment. However, next-generation vehicles, which are both automated and connected to digital networks, bring qualitative changes in the collection and storage of data, well beyond what is covered in existing Right to Repair agreements (Kessler 2017). While the contentions over car data have heretofore focused on repair codes, the mappings produced by self-driving cars are made of data captured from their surroundings, including people, places, and communications along their path. The contentious history of Google cars intercepting wifi communications while capturing Street View images highlights the implications of this emerging technological debate for privacy and security, among other fundamental issues (Burdon and McKillop 2013).

The experience of the Right to Repair movement, and legislation it has pushed in the United States, illustrates that it is possible to open the closed informational environments that have come to dominate digital capitalism. The Right to Repair addresses a fundamental imbalance of data access between manufacturers, on the one hand, and consumers and third-party service providers, on the other hand. However, the data collected by connected and automated vehicles are both harder to access by non-authorized parties (as they circulate through closed networks under manufacturer control), and more valuable for purposes beyond car repair. Indeed, as cars come to rely completely on a vast array of sensors for navigation, the possibilities for profit multiply through the marketization of collected data about user habits, preferences, identity, locations, routes, and surroundings, as well as subscription services such as navigation guidance, emergency assistance, and onboard entertainment systems. This portends a more thorough reconfiguration of spatial information (and space itself) towards the logic embedded in applications like Yelp and

2. These are: Washington, Massachusetts, Vermont, New York, Hawaii, Illinois, Iowa, Kansas, Minnesota, Missouri, North Carolina, Nebraska, New Hampshire, New Jersey, Oklahoma, Tennessee, Virginia, and California.

Google Maps, which are designed to facilitate consumption in, and of, space, as a primary activity.

In this respect, the Right to Repair presents an avenue that addresses the data pipeline of the car only inasmuch as it concerns the repair of the vehicle itself. Yet, with cars becoming increasingly sophisticated collections of computers, “car repair” only covers what is already a shrinking aspect of the car data environment. In fact, automated vehicles are no longer merely cars, but are instead, as one commentator has called them, “data harvesting machines” that are connected to a diverse assortment of services (Kaminska 2017). In turn, these data harvesting machines rely on spatial representations to navigate space, while creating economic value out of such representations, and potentially transforming space itself in the process. In this emerging environment of pervasively commodified spatial data flows, it is necessary to have a more open and deliberative process informing the public what data are collected by automated vehicles, what is done with said data, and who can appropriate and profit from them.

As Right to Repair movements and legislation have already demonstrated, grassroots movements can be successful in exerting the pressure necessary to open the closed data pipelines under corporate control. While initially this success has been aimed at repair activities, more attention should be directed to tracing the flows of vehicle data and accounting for their expanding uses and applications. In particular, as increasingly automated cars come to rely on complex mappings to navigate, the process of how these are assembled and commodified should be made transparent and open for public deliberation. Concomitant with lobbying efforts for new legislation on this front, below I discuss the possibilities presented by two additional avenues of potential intervention: design and hacking.

## DESIGN

Udacity is an online, STEM-focused, education company co-founded by Sebastian Thrun, who led the development of the Google self-driving car and won the 2005 DARPA Grand Challenge—the foremost competition of autonomous vehicles, funded by the US Department of Defense. Udacity’s aim is to prepare students for jobs in the information technology industry. Given this focus, and the interests of its founders, one of the first courses it offered was titled “Building a Robotic Car,” taught by Thrun in 2012.

This has expanded into a “nanodegree” entirely devoted to providing students with skills to “complete the journey to a Self-driving Car career” (Udacity 2017).

In parallel to expanding the formal courses and certificates focused on self-driving cars, Udacity is building its own version of this technology as an open source project. After outfitting a 2016 Lincoln MKZ with lidar, radar, cameras, and other equipment, Udacity configured the Robot Operating System (ROS), and opened the code “to build and refine an open source self-driving car with the help of students from around the world” (Cameron 2016). This project consists of various discrete tasks, which address individual components of the autonomous vehicle, and are open for public participation. The code is managed through a GitHub repository, and users can communicate through the Slack messaging platform, using an account dedicated to this project. At the time of this writing, the open source project page on the Udacity website ([udacity.com/self-driving-car](https://udacity.com/self-driving-car)) redirects to the Self-driving Car Nanodegree page, suggesting a pivot back to the company’s core mission of selling online educational services.

While Udacity has leveraged its partnerships with top academic institutions such as Stanford and Carnegie Mellon, as well as leading companies in the automobile (Mercedes-Benz, Honda), ride-sharing (Uber), and information technology (IBM, Nvidia) industries to entice students with an inside track into high-paying engineering jobs, another open source self-driving car initiative is developing on the outside of this environment, and with a different set of goals: the Open-Source Self-driving Car Initiative, or OSSDC ([ossdc.org](https://ossdc.org)). The differences between these two open source projects are illustrative of the range of orientations that can develop through open source projects, and can point to the possibility of future initiatives explicitly aimed at critiquing and contesting the collection, use, and commodification of self-driving car data.

Marius Slaveșcu, a Toronto-based inventor, started the Open-Source Self-driving Car Initiative in 2016 after he joined Udacity’s Open Source Self-driving Car Challenges. According to OSSDC’s Mission and Vision statement, this initiative was created, “to bring together the best open source technologies and open research to allow anyone (not only experts) build affordable self-driving cars and autonomous mobile robots in a DIY manner [*sic*], from toy size (RC cars) to full size (full size cars)”

(Slavescu 2017b; 2017c). The basic structure of OSSDC largely mirrors that of Udacity's project: code is shared through a GitHub repository, and communication between members takes place through Slack. While OSSDC is still in its infancy, and many of its core components are in flux (such as its website, which is still missing important content, or its logo—an upside down car that is the topic of much discussion by contributors), its divergence from the corporate orientation of Udacity (as a feeder for the self-driving car industry) has been made clear from the outset. For example, in the context of a discussion about the design specifications of the logo for OSSDC, Slavescu expanded on his outlook for the orientation of this initiative, explicitly looking to transcend commercial goals:

I'm looking for people that really want to contribute to Open Source Self-driving Car Initiative, and make it applicable to many SDC and robotics projects, instead of just looking to build next Uber (not that is anything wrong with that [*sic*]).

In my opinion, OSSDC.org is an organization that should be a model for the future, where people join to Learn, Teach, Invent, Make, participate and contribute their expertise [*sic*] in open ways (through OSSDC GitHub Organization), for the good of everyone, not just for their employees or investors. (Slavescu 2017a)

Whether OSSDC will survive with this outlook (if at all), or mutate to adopt a different ethos, is too soon to tell. However, this initiative's existence illustrates a viable form of non-commercial organization to tackle the development of an emerging and particularly complex technology. On the other hand, OSSDC also exemplifies, through its tentative beginnings and lack of clear organization, the difficulties of existing and expanding in the self-driving car technology environment without the explicit support from, or integration into, a corporate pipeline.

As shown by Udacity, opening the code and development of a self-driving car can be beneficial in identifying potential job candidates for the industry, and even developing innovative technological solutions through collaboration.

This strategy has also been embraced by Baidu, the leading search engine in China, which has taken it one step further. Baidu has announced the gradual opening of its entire self-driving technology stack, named Project Apollo, starting in a limited environment in 2017 and releasing full self-driving software by 2020 (Muoio 2017). In this case, Baidu's goal is to drive the development of the self-driving car industry through community input, while retaining the position to commercialize a finished product.

The different strategies embraced by Baidu and Udacity, on the commercial side, and OSSDC on the not-for-profit side, illustrate how the emerging landscape of self-driving cars is colored by the enormous economic rewards promised by this technology. While open source as a practice has the potential to disrupt asymmetric power arrangements in the self-driving car environment, it can also be leveraged as a strategy to reinforce them. OSSDC is meaningful as precedent for a self-organized open source initiative focused on self-driving cars. Yet, it does not directly address the issues surrounding collection, use, and appropriation of data by these vehicles. This is particularly important in the context of the pervasive, multimodal data collection enabled by automated vehicles. Open source design can offer a window into understanding, critiquing, and checking the specific mechanisms by which these vehicles capture highly granular, personal (and potentially illegal) data on location, routes, and user behavior, and integrate them into virtual spatial representations.<sup>3</sup> Such a window would provide the opportunity for public scrutiny into concerns central to the deployment of self-driving cars, such as the relationship between a vehicle's software, data, and technological configuration, on the one hand, and the assessment of questions of liability, reliability, and safety, on the other. It is through the window offered by open source design that potential counter-mappings can then advance alternative spatial representations.

Thus, in a similar way that targeted movements are required to promote legislation that explicitly addresses the power asymmetries shaping the self-driving car data pipeline, new open source initiatives will have to emerge that are geared towards demanding data transparency, proposing alternative technologies, and building frameworks for contestation. An element that can position open source initiatives as an alternative, and counter, to the

3. Many of the data collection methods that are present in self-driving cars have previously been subject to litigation and government investigation in the US and various European countries during their deployment by Google Street View vehicles—in particular the collection of Wi-Fi network data along photographed routes. For an overview of these cases, see Blitz (2012), Electronic Privacy Information Center (2010), and Geissler (2012).

corporate-dominated self-driving car ecosystem, is hacking. Both as a technical practice, and an ethic of disruption, hacking can be an avenue for critiques of self-driving car development, as well as a tool to open the black boxes of technical and corporate control that contain the data collected by self-driving cars. In the next subsection, I examine two recent instances of automated vehicle hacking and explore how these can be used to inform a counter-mapping movement in the context of self-driving cars.

## HACKING

In 2015, Charlie Miller, a security researcher at Twitter, and Chris Valasek, Director of Vehicle Security at the information security firm IOActive, remotely hacked the computers of a 2014 Jeep Cherokee, gaining control of the vehicle's steering, transmission, and brakes. This was a significant leap from their hacking of a Toyota Prius and a Ford Escape in 2013, which took place with their computers physically connected to the cars' onboard diagnostic ports (Greenberg 2015). The progression towards wireless hacking is both indicative of the auto industry's trend of making vehicles more connected, and a serious warning ahead of the massive deployment of fleets of networked autonomous vehicles. Miller and Valasek shared their findings with Fiat Chrysler, the maker of Jeep Cherokee, and published a comprehensive guide exposing its security vulnerabilities (Miller and Valasek 2015), with the aim of alerting automakers of the potential security flaws while simultaneously putting pressure on them by stoking public opinion.

In the process of remotely hacking into the Jeep Cherokee, Valasek and Miller relied on the car computer's capabilities of communication, location, and automation, and exploited their vulnerabilities over cellular data networks (Miller and Valasek 2015). Through this exercise, they showed that, by gaining access to a vehicle, hackers can directly manipulate its trajectory and actions, as well as track its user's movement patterns, location, and behavior from long distances. While this is already a significant issue due to the large number of digitally connected vehicles in the market, the widespread adoption of autonomous vehicles will only worsen the implications for privacy, cyber-security, and public safety.

The work of Valasek and Miller, though initially downplayed by auto manufacturers, has gained the attention of

some US legislators, who have proposed legislation specifically aimed at addressing the flaws exposed by remote vehicle exploitation. The Security and Privacy in Your Car (SPY Car) Act of 2015 was sponsored by Senator Ed Markey, with the aim of

[directing] the National Highway Traffic Safety Administration (NHTSA) to conduct a rulemaking to issue motor vehicle cybersecurity regulations that require motor vehicles manufactured for sale in the United States to protect against unauthorized access to: (1) electronic controls or driving data, including information about the vehicle's location, speed, owner, driver, or passengers; or (2) driving data collected by electronic systems built into a vehicle while that data is stored onboard the vehicle, in transit from the vehicle to another location, or subsequently stored or used off-board the vehicle. The regulations must require vehicles with accessible data or control signals to be capable of detecting, reporting, and stopping attempts to intercept such driving data or control the vehicle. (Security and Privacy in Your Car Act 2015)

The bill was read twice on the Senate floor and eventually referred to the Committee on Commerce, Science, and Transportation. Two years later, in 2017, Senator Markey reintroduced the bill, which to date has repeated its path through the Senate, having been referred to the same Committee, where it remains. Thus, while many legislators have stated that vehicle cybersecurity is a top priority, to date no new legislation has materialized (Armerding 2017). Episodes of remote vehicle hacking, such as that carried out by Miller and Valasek, or the Tesla car hacks in 2016 and 2017 by researchers from Keen Security Lab, part of Chinese technology leader Tencent (Weise 2017), have informed legislative discussions on improving security by pinpointing specific, and exploitable, flaws. However, the slow legislative pace and the competition between automakers towards increasingly interconnected vehicles constitute serious obstacles to a more secure environment. Furthermore, these hacking instances demonstrate the importance of location data, as well as other forms of spatial data collected and processed by cars, since they can be used (among other applications) to identify, as well as disrupt and control the movements—and potentially the safety—of car passengers.



In another instance of hacking that has significant ramifications for self-driving cars, George Hotz (who became famous for being the first person to “jailbreak” an iPhone in 2007) recently pioneered an open source self-driving platform called *openpilot* (spelled in lowercase on their GitHub page, [github.com/commaai/openpilot](https://github.com/commaai/openpilot)). With the help of a smartphone, this platform can enhance existing car systems (such as lane detection and assisted parking), endowing them with “semi self-driving” capabilities. Developed through Hotz’s company, *comma.ai* (also lowercase), the platform was originally set to be an aftermarket kit, commercially available for \$999 USD. However, after receiving a letter from the National Highway Traffic Safety Administration, which threatened fines for selling untested self-driving technology to the public, Hotz decided to release it publicly as open code (Zaleski 2107). While Hotz has stressed the research purposes of this release, he has also outlined a commercial strategy for *openpilot*, which distances itself from the hardware, and focuses on the data network underlying self-driving cars:

Hotz compared *Open Pilot* [*sic*] to Android, and said that it’s really aimed at “hobbyists and researchers and people who love” self-driving technology. “It’s for people who want to push the future forward,” he said. When asked how or if *Comma.ai* [*sic*] plans to make any money off of this project, Hotz responded: “How does anybody make money? Our goal is to basically own the network. We want to own the network of self-driving cars that is out there.” (O’Kane and Goode 2016)

In effect, if adopted massively, *openpilot* would assist people in hacking into their own vehicles for the purpose of transforming them into (at least-partial) self-driving cars and connect them to a network of car data flows that *comma.ai* would be in a position to monetize. To this end, the next iteration of *comma.ai*’s efforts has been the development of a “decoder” that lets users monitor and interpret the data collected by their cars. The goal is to “democratize access to the decoder ring for your car” (*comma.ai* 2017). According to Hotz, his technology gives users access to all the same car data that manufacturers can access, from fuel use, to RPMs, to driver behavior—thus leveling the playing field and allowing individuals to train their own self-driving cars. As cars become increasingly autonomous, this type of technology can potentially allow users

to examine the data pipeline that feeds into the mappings underpinning automated navigation. This, in turn, can empower individuals, user communities, grassroots organizations, or regulators to construct alternative narratives, arguments, and representations in order to hold car manufacturers accountable, demand transparency, or check the quality of the data-driven services they receive. On the other hand, a more open car data environment can also expose existing security vulnerabilities in networked and automated systems, or even create new ones that endanger the users of such technologies and the public in general.

Yet, while giving users the tools to view and interpret their vehicle’s data may constitute, in and of itself, a democratic exercise in the eyes of Hotz, it is fully subordinated to the logic of an emerging market for car data. Not coincidentally, *comma.ai*’s innovations are well positioned to successfully exploit the potential profits from said market. As he suggested in a recent interview with the libertarian outlet *Reason*, Hotz’s idea of openness is characterized by a form of collective sharing that comes with a profit imperative; this imperative is necessarily fulfilled through market action:

I don’t want to have a monopoly on data. This is the old way of thinking. What if we could open our data up more, and really think about it, not as like, “Facebook owns this data, Google owns this data,” but we all collectively own the data and you’re contributing to a big collective pool of data. . . . Now it’s a market, it’s not like, “Oh we’re all going to do this for smiles and roses,” or whatever communists have, but no we’re going to do it for you know, [inaudible] the market. Create this data, contribute to this, all the data combined is a whole lot more powerful than any piece of the data alone and I think we can do incredible things with these sort of data sets, right? (Monticello 2017)

The double-edged sword of empowering users to access and interpret their own vehicle data, while creating a market for it, exemplifies one of the defining tensions of digital capitalism. Therefore, in light of technological advances, such as those put forth by *comma.ai* and various other open source initiatives, a fuller political economic examination of self-driving car data must be conducted. This examination should read the dynamics of legislation,

open source design, and hacking (among other elements) in a political economic context that considers the power asymmetries and monetary incentives inherent to the entire self-driving car ecosystem, and its integration into digital capitalism. It is only through such analysis that we

can have both a clearer understanding of how new data spaces are being created inside self-driving vehicles, how they contribute to reshaping the physical and social world, and how we can build initiatives that question, regulate, and open this process to public deliberation.

## COUNTER-MAPPING THE DATA SPACES OF AUTONOMOUS DRIVING

AS AUTONOMOUS VEHICLES CONTINUE to improve, they are raising important questions of ownership, security, privacy, liability, and even competition. Yet, the conversations around this innovation and its consequences have so far been centered on the cars themselves, as well as the technologies that can allow them to become autonomous. This is for good reason, since the widespread deployment of self-driving cars has enormous societal consequences, the most immediate of which have to do with how safely they perform on the roads. However, underlying—and enabling—this technological development, is an emerging data ecosystem generated by the massive collection of fine-grained vehicle data about the cars themselves as well as the landscape they navigate, and even the users that drive them. This data ecosystem—much of which is assembled into highly complex mappings through lidar point clouds, photography, GPS-enabled navigation, image recognition, and other technologies—constitutes a core component of the political economy of automated vehicles.

Self-driving cars constitute an extension of an established industry—the automobile industry—into digital capitalism through intensified exchanges with other cutting-edge industries such as those of information, geospatial technologies, and robotics. On the other hand, the structures underpinning the collection, use, and monetization of data harvested by self-driving cars are made in the crucible of the digital economy. The business models of Google and Facebook shape the emerging autonomous vehicle data ecosystem to a greater degree than existing strategies of the automobile industry. Bringing cars into a digital, networked environment of monetized data flows realigns the auto industry's economic incentives and articulations of power with broad ramifications. The emerging automated navigation landscape is assembled through new configurations that include both incumbents and new entrants across information, robotics, geospatial, automobile, and other technology industries, along with subnational and

national authorities across various countries, grassroots organizations, and communities of users.

As the previous sections illustrated, the development and deployment of autonomous vehicles raises, among others, important questions about ownership, privacy, and security—of vehicles, as well as data (with an increasing emphasis on spatial data). Consequently, new movements and initiatives, spanning a number of domains, are contesting the closed structures of access and ownership upon which the automated vehicle order is premised. However, as the Right to Repair movement and legislation in the US also show, while these have achieved success in pushing back against restrictive practices from automakers, they have done so in large part because this pushback is aligned with the interests of another powerful industry, which is that of the aftermarket for car products and repair services. A similar situation can be seen in the open source movement for self-driving cars, where the leading initiatives are those that are either training people for employment in the self-driving car industry (such as Udacity), or using open source as a new strategy for technological innovation and ensuring a leading position in the market (Baidu).

While hacking can potentially bring more agency to users and mobilize regulation aimed at increasing security, transparency, and accountability of manufacturers, these same practices can pose important security risks to drivers, pedestrians, and the public in general. Public infrastructure can be endangered, and hackers can potentially compromise sensitive information while feeding underground data markets. Yet, in spite of these significant implications, legislation on this front has so far been stalled, while the most dynamic hacking initiatives (such as Geoge Hotz's openpilot) are—in Facebook-speak—“moving fast and breaking things,” embracing the liberating rhetoric of open source and spurred by the promise of rewards from a leading market position to monetize car data flows. This

should be no surprise, given the system of incentives that undergirds digital capitalism, which privileges innovation over security, and monetization over privacy and other users' rights. As Miller and Valasek's car hacking demonstrations have shown, the race for automated navigation leads automakers to compete over the release of new technical features, and new revenue streams, while paying secondary attention to the possible negative externalities for consumers.

Carefully assessing the risks brought by each of these avenues, I suggest that we can also explore their potential to open the black boxes of autonomous driving under the umbrella of counter-mapping. This can encompass, through a self-reflective approach, the technical analysis, the ethics of contestation, and the construction of alternatives necessary to provide a much-needed counterbalance to the capitalist imperative driving the self-driving car industry. In particular, it is essential to open for public debate, and

achieve a broader understanding of, how autonomous vehicles re-create and navigate space. This is crucial because the mappings underlying autonomous navigation are also the mappings underlying potential transformations of space, since the rise of self-driving cars cannot be divorced from the economic logics and incentives that define digital capitalism, nor can it be understood separately from the technocratic promises (and perils) of the corporate-driven smart city rhetoric (Luque-Ayala and Marvin 2015; Wiig 2015). This ongoing counter-mapping can involve a critique and a re-creation of the virtual spaces made by (and for) autonomous navigation. Attending to the data spaces collected by cars (as they become "data harvesting machines") and tracing how these data spaces are assembled, used, and appropriated, counter-mapping can provide an integrative perspective that allows us to consider, monitor, and deliberate over the entire data ecosystem, while identifying opportunities for concerted political action.

## CONCLUSION

AS COUNTER-MAPPING HAS SHOWN in instances ranging from indigenous land claims to data privacy, the structures of power underlying technological and informational paradigms can be contested by turning these paradigms' mapping technologies onto themselves. Counter-mapping, as an ethos and an evolving set of practices, can achieve this by developing in parallel to the very tools used by those actors who have the power to "map." The epistemological and political tasks enabled by counter-mapping are thus necessary to hold mapping powers to account precisely because mapping is not just a representation of particular visions of the world, but also a means of enacting them. In this respect, the mappings performed by autonomous vehicles not only create a vision of the world suitable for navigation, but also for the capital imperative of monetizing those spatial representations. Beyond this, once massively deployed and adopted, autonomous cars could have the power to reproduce their internal spatial representations onto the physical world by exerting change on transportation systems, flows of capital, industrial organization, policymaking priorities, and social practices.

In light of these vast ramifications, it is imperative to develop strategies to critically examine the production of space within autonomous vehicles, and open up this process for wider participation. I have argued here that counter-mapping represents an integrative perspective that can incorporate several avenues through which autonomous vehicle data collection, use, and appropriation can be critiqued and contested. Legislation, open source design, and hacking represent a subset of the potential avenues for counter-mapping the data spaces produced and networked by autonomous vehicles. However, each of these has to be critically evaluated for how they are positioned with respect to the systems of incentives that structure digital capitalism. Mobilizing these practices for the purposes of contestation requires a pushback against the imperatives towards profit and corporate control that so often shape their trajectory. Counter-mapping, as an ethos and an evolving set of practices, can thus contribute to the building of alternatives to the black-boxed construction of new data spaces, often hidden from public input and deliberation, and which underpin what is often advertised as the inevitable, automated, order of things to come.

## REFERENCES

- An Act Relative to Automotive Repair. 2013. 2013 Massachusetts Acts 165.
- Armerding, Taylor. 2017. "Congress Looks to Take the Wheel on Autonomous Vehicles." *Naked Security*, August 7, 2017. <https://nakedsecurity.sophos.com/2017/08/07/congress-looks-to-take-the-wheel-on-autonomous-vehicles/>.
- Bassett, Mike. 2016. "Revisiting the Right to Repair." *24x7 Magazine*, March 3, 2016. <http://www.24x7mag.com/2016/03/revisiting-right-to-repair/>.
- Bergen, Mark. 2018. "Nobody Wants to Let Google Win the War for Maps All Over Again." *Bloomberg*, February 21, 2018. <https://www.bloomberg.com/news/features/2018-02-21/nobody-wants-to-let-google-win-the-war-for-maps-all-over-again>.
- Bissell, David. 2018. "Automation Interrupted: How Autonomous Vehicle Accidents Transform the Material Politics of Automation." *Political Geography* 65: 57–66. doi: [10.1016/j.polgeo.2018.05.003](https://doi.org/10.1016/j.polgeo.2018.05.003).
- Blitz, Marc Jonathan. 2012. "The Right to Map (and Avoid Being Mapped): Reconceiving First Amendment Protection for Information-Gathering in the Age of Google Earth." *Columbia Science and Technology Law Review* 14: 115–202.
- Boeglin, Jack. 2015. "The Costs of Self-Driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation." *Yale Journal of Law and Technology* 17: 171–204.
- Brodsky, Jessica S. 2016. "Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit the Brakes on Self-Driving Cars." *Berkeley Technology Law Journal* 31: 851–878.
- Burdon, Mark, and Alissa McKillop. 2013. "The Google Street View Wi-Fi Scandal and Its Repercussions for Privacy Regulation." *Monash University Law Review* 39 (3): 702–738.
- Cameron, Oliver. 2016. "We're Building an Open Source Self-Driving Car." *Medium*, September 29, 2016. <https://medium.com/udacity/were-building-an-open-source-self-driving-car-ac3e973cd163>.
- Casas-Cortés, Maribel, Sebastian Cobarrubias, Charles Heller, and Lorenzo Pezzani. 2017. "Clashing Cartographies, Migrating Maps: The Politics of Mobility at the External Borders of E.U.Rope." *ACME* 16 (1): 1–33.
- Cattoor, Bieke, and Chris Perkins. 2014. "Re-Cartographies of Landscape: New Narratives in Architectural Atlases." *The Cartographic Journal* 51 (2): 166–178. doi: [10.1179/1743277413Y.0000000076](https://doi.org/10.1179/1743277413Y.0000000076).
- comma.ai. 2017. "A Panda and a Cabana: How to Get Started Car Hacking with comma.ai." *Medium*, July 7, 2017. [https://medium.com/@comma\\_ai/a-panda-and-a-cabana-how-to-get-started-car-hacking-with-comma-ai-b5e46fae8646](https://medium.com/@comma_ai/a-panda-and-a-cabana-how-to-get-started-car-hacking-with-comma-ai-b5e46fae8646).
- Counter Cartographies Collective, Craig Dalton, and Liz Mason-Deese. 2012. "Counter (Mapping) Actions: Mapping as Militant Research." *ACME* 11 (3): 439–466.
- Cugurullo, Federico. 2018. "Exposing Smart Cities and Eco-Cities: Frankenstein Urbanism and the Sustainability Challenges of the Experimental City." *Environment and Planning A: Economy and Space* 50 (1): 73–92. doi: [10.1177/0308518X17738535](https://doi.org/10.1177/0308518X17738535).
- Dalton, Craig M., and Tim Stallmann. 2017. "Counter-Mapping Data Science." *The Canadian Geographer / Le Géographe Canadien* 61 (1): 93–101. doi: [10.1111/cag.12398](https://doi.org/10.1111/cag.12398).
- Electronic Privacy Information Center. 2010. "Investigations of Google Street View." <https://epic.org/privacy/streetview/>.
- Evans, Benedict. 2017. "Winner-Takes-All Effects in Autonomous Cars." *Benedict Evans*, August 22, 2017. <https://www.ben-evans.com/benedictevans/2017/8/20/winner-takes-all>.

- Gao, Paul, Russell Hensley, and Andreas Zielke. 2014. "A Road Map to the Future for the Auto Industry." *McKinsey & Company*. <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/a-road-map-to-the-future-for-the-auto-industry>.
- Geissler, Roger C. 2012. "Private Eyes Watching You: Google Street View and the Right to an Inviolable Personality." *Hastings Law Journal* 63: 897–926.
- Gieseeking, Jen Jack. 2016. "Crossing over into Neighbourhoods of the Body: Urban Territories, Borders and Lesbian-Queer Bodies in New York City." *Area* 48 (3): 262–270. doi: [10.1111/area.12147](https://doi.org/10.1111/area.12147).
- Greenberg, Andy. 2015. "Hackers Remotely Kill a Jeep on the Highway—With Me in It." *Wired*, July 21, 2015. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.
- Harris, Leila M., and Helen D. Hazen. 2005. "Power of Maps: (Counter) Mapping for Conservation." *ACME* 4 (1): 99–130.
- Hook, Leslie, and Ian Bott. 2018. "Driverless Cars: Mapping the Trouble Ahead." *Financial Times*, February 21, 2018. <https://www.ft.com/content/2a8941a4-1625-11e8-9e9c-25c814761640>.
- Kaminska, Izabella. 2017. "Your Car as a Data Harvesting Machine." *Financial Times*, November 24, 2017. <http://ftalphaville.ft.com/2017/11/24/2196085/your-car-as-a-data-harvesting-machine/>.
- Kessler, Sarah. 2017. "The Connected Car of the Future Could Kill off the Local Auto Repair Shop." *Quartz*. <https://qz.com/1054261/the-connected-car-of-the-future-could-kill-off-the-local-auto-repair-shop/>.
- Kitchin, Rob. 2014. *The Data Revolution*. Los Angeles: SAGE.
- Krueger, Rico, Taha H. Rashidi, and John M. Rose. 2016. "Preferences for Shared Autonomous Vehicles." *Transportation Research Part C: Emerging Technologies* 69: 343–355. doi: [10.1016/j.trc.2016.06.015](https://doi.org/10.1016/j.trc.2016.06.015).
- Lanctot, Roger. 2018. "Accelerating the Future: The Economic Impact of the Emerging Passenger Economy." Boston, MA: Strategy Analytics. [https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf?cid=em-elq-26916&utm\\_source=elq&utm\\_medium=email&utm\\_campaign=26916&elq\\_cid=1494219](https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf?cid=em-elq-26916&utm_source=elq&utm_medium=email&utm_campaign=26916&elq_cid=1494219).
- Lipson, Hod, and Melba Kurman. 2016. *Driverless: Intelligent Cars and the Road Ahead*. Cambridge MA: MIT Press.
- Luque-Ayala, Andrés, and Simon Marvin. 2015. "Developing a Critical Understanding of Smart Urbanism." *Urban Studies* 52 (12): 2105–2116. doi: [10.1177/0042098015577319](https://doi.org/10.1177/0042098015577319).
- Manauagh, Geoff. 2016. "Robot War and the Future of Perceptual Deception." *BLDGBLOG*, July 5, 2016. <http://www.bldgblog.com/2016/07/robot-war-and-the-future-of-perceptual-deception/>.
- Mattern, Shannon. 2017. "Mapping's Intelligent Agents." *Places Journal*, September 2017. doi: [10.22269/170926](https://doi.org/10.22269/170926).
- Mayer-Schönberger, Viktor, and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. New York: Houghton Mifflin Harcourt.
- Metzger, Andy. 2017. "Proposal Expands 'Right to Repair' Movement to Electronics in Mass." *Telegram.com*, September 27, 2017. <http://www.telegram.com/news/20170927/proposal-expands-right-to-repair-movement-to-electronics-in-mass>.
- Miller, Charlie, and Chris Valasek. 2015. "Remote Exploitation of an Unaltered Passenger Vehicle." *IOActive*. [https://ioactive.com/pdfs/IOActive\\_Remote\\_Car\\_Hacking.pdf](https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf).
- Monticello, Justin. 2017. "Super Hacker George Hotz: I Can Make Your Car Drive Itself for Under \$1,000." *Reason.com*, October 27, 2017. <http://reason.com/video/george-hotz-self-driving-autonomous-car>.

- Muoio, Danielle. 2017. "A Chinese Internet Giant Just Made a Big Move to Compete with Tesla in the Self-Driving-Car Space." *Business Insider*, April 19, 2017. <http://www.businessinsider.com/baidu-will-open-source-self-driving-car-software-2017-4>.
- Peluso, Nancy Lee. 1995. "Whose Woods Are These? Counter-mapping Forest Territories in Kalimantan, Indonesia." *Antipode* 27 (4): 383–406. doi: [10.1111/j.1467-8330.1995.tb00286.x](https://doi.org/10.1111/j.1467-8330.1995.tb00286.x).
- O’Kane, Sean, and Lauren Goode. 2016. "George Hotz Is Giving Away the Code behind His Self-Driving Car Project." *The Verge*, November 30, 2016. <https://www.theverge.com/2016/11/30/13779336/comma-ai-autopilot-canceled-autonomous-car-software-free>.
- Perzanowski, Aaron, and Jason Schultz. 2016. *The End of Ownership: Personal Property in the Digital Economy*. Cambridge, MA: MIT Press.
- Propen, Amy D. 2005. "Critical GPS: Toward a New Politics of Location." *ACME* 4 (1): 131–144.
- Schlossberg, Marc, Adam Millard-Ball, Elizabeth Shay, and William (Billy) Riggs. 2018. "Rethinking the Street in an Era of Driverless Cars." *Urbanism Next*. <https://scholarsbank.uoregon.edu/xmlui/handle/1794/23331>.
- Security and Privacy in Your Car Act. 2015. S. Res. 1806, 114<sup>th</sup> Cong.
- Shelton, Taylor, Matthew Zook, and Alan Wiig. 2015. "The 'Actually Existing Smart City.'" *Cambridge Journal of Regions, Economy and Society* 8 (1): 13–25. doi: [10.1093/cjres/rsu026](https://doi.org/10.1093/cjres/rsu026).
- Slavescu, Marius. 2017a. "Thanks Miguel A." *Medium*, April 23, 2017. <https://medium.com/@mslavescu/thanks-miguel-a-2434929a8187>.
- . Marius. 2017b. "What is Next in OSSDC.Org?" *Becoming Human*, April 7, 2017. <https://becominghuman.ai/what-is-next-in-ossdc-org-3610f75794f3>.
- . 2017c. *OSSDC-Hacking-Book*. Open Source Self Driving Car Initiative. <https://github.com/OSSDC/OSSDC-Hacking-Book>.
- Stilgoe, Jack. 2018. "Machine Learning, Social Learning and the Governance of Self-Driving." *Social Studies of Science* 48 (1): 25–56. doi: [10.1177/0306312717741687](https://doi.org/10.1177/0306312717741687).
- Udacity. 2017. "Self-Driving Car Nanodegree | Udacity." Accessed December 3, 2017. <https://www.udacity.com/course/self-driving-car-engineer-nanodegree--nd013>.
- Wainwright, Joel, and Joe Bryan. 2009. "Cartography, Territory, Property: Postcolonial Reflections on Indigenous Counter-Mapping in Nicaragua and Belize." *Cultural Geographies* 16 (2): 153–178. doi: [10.1177/1474474008101515](https://doi.org/10.1177/1474474008101515).
- Weise, Elizabeth. 2017. "Chinese Group Hacks a Tesla for the Second Year in a Row." *USA Today*, July 27, 2017. <https://www.usatoday.com/story/tech/2017/07/28/chinese-group-hacks-tesla-second-year-row/518430001>.
- Wiig, Alan. 2015. "IBM’s Smart City as Techno-Utopian Policy Mobility." *City* 19 (2–3): 258–273. doi: [10.1080/13604813.2015.1016275](https://doi.org/10.1080/13604813.2015.1016275).
- . 2018. "Secure the City, Revitalize the Zone: Smart Urbanization in Camden, New Jersey." *Environment and Planning C: Politics and Space* 36 (3): 403–422. doi: [10.1177/2399654417743767](https://doi.org/10.1177/2399654417743767).
- Zaleski, Andrew. 2017. "This Man Wants To Open Source Your Car." *Fortune*, August 23, 2017. <http://fortune.com/2017/08/23/george-hotz-comma-ai>.

