Surveillance & Society

Article

From Banal Surveillance to Function Creep: Automated License Plate Recognition (ALPR) in Denmark

Gabriel Pereira

London School of Economics and Political Science, UK
gabrielopereira@gmail.com

Christoph Raetzsch

Aarhus University, Denmark
craetzsch@cc.au.dk

Abstract

This article discusses how Automated License Plate Recognition (ALPR) has been implemented in Denmark across three different sectors: parking, environmental zoning, and policing. ALPR systems are deployed as a configuration of cameras, servers, and algorithms of computer vision that automatically reads and records license plates of passing cars. Through digital ethnography and interviews with key stakeholders in Denmark, we contribute to the fields of critical algorithm and surveillance studies with a concrete empirical study on how ALPR systems are configured according to user-specific demands. Each case gives nuance to how ALPR systems are implemented: (1) how the seamless charging for a "barrier-free" parking experience poses particular challenges for customers and companies; (2) how environmental zoning enforcement through automated fines avoids dragnet data collection through customized design and regulation; and (3) how the Danish Police has widened its dragnet data collection with little public oversight and questionable efficacy. We argue that ALPR enacts a form of "banal surveillance" because such systems operate inconspicuously under the radar of public attention. As the central analytic perspective, banality highlights how the demand for increasing efficiency in different domains makes surveillance socially and politically acceptable in the long run. Although we find that legal and civic modes of regulation are important for shaping the deployment of ALPR, the potential for function creep is embedded into the very process of infrastructuring due to a lack of public understanding of these technologies. We discuss wider consequences of ALPR as a specific and overlooked instance of algorithmic surveillance, contributing to academic and public debates around the embedding of algorithmic governance and computer vision into everyday life.

Introduction

"Banality is the fatality of our modern world." (Baudrillard qtd. in Gane 1993: 45)

In July 2020, mysterious cameras were set up on a busy commuter road in central Aarhus, Denmark. Concerned about such unknown technology surveilling the neighborhood, a citizen inquired with the city's infrastructure councilor, but there was no response. The local newspaper, *Aarhus Stiftstidende*, began to investigate, but neither the Danish Road Directorate nor the local police department immediately knew what the cameras were doing there. As it later turned out, the cameras had been installed by the Danish Environmental Protection Agency in partnership with the state-owned company Sund & Bælt to enforce environmental zoning against polluting vehicles. These mysterious cameras, known as Automated License Plate Recognition (ALPR) cameras,[1] were only the most visible part of an infrastructure consisting of onsite cameras, network connections, algorithms, databases, and analytics facilities. They are often taken for speed

[1] In this article, we use American nomenclature (ALPR, license plate), as opposed to the British (ANPR, number plate) or the Danish (ANPG, Automatisk Nummerpladegenkendelse, nummerplade).

Pereira, Gabriel, and Christoph Raetzsch. 2022. From Banal Surveillance to Function Creep: Automated License Plate Recognition (ALPR) in Denmark. *Surveillance & Society* 20 (3): 265-280.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

cameras by car drivers, but their purpose and setup reach new levels of integration for surveillance technologies.

In this article, we offer an empirical study of how ALPR systems are currently deployed in Denmark in three distinct domains: parking, environmental zoning, and policing. We critically discuss the process of infrastructuring as a form of banal surveillance, highlighting modes of sociotechnical surveillance that are inconspicuous and tacitly accepted for seemingly beneficial purposes. Capturing a license plate may appear to be a less personal mode of surveillance than facial recognition or social media analytics. However, despite its seemingly banal dimensions, there is no opting out from such surveillance because many car drivers are not aware of being automatically registered by ALPR systems (Selinger and Hartzog 2019; Smith 2020). Our goal is to draw attention to these inherent dynamics of infrastructuring for banal surveillance: how ALPR gets developed and deployed in pervasive systems that operate as information infrastructures (see Star 1999; Star and Ruhleder 1996; Raetzsch et al. 2019). We adopt the notion of "infrastructuring" to focus on the ongoing processes that shape constellations of technologies, actors, and use cases, and that demonstrate problematic aspects emerging from such configurations.

The perspective of banal surveillance emphasizes three aspects in relation to ALPR. First, it draws attention to the processes in which infrastructures are developed and become embedded into quotidian usage, contributing to a "mundanization of automated decision-making" (Kaun 2021) and an "integration of surveillance in the everyday" (Bellanova, De Hert, and Gutwirth 2010: 48, our translation). Second, these systems work as combinations of visible infrastructural components (e.g., cameras, networks) with less visible ones (e.g., algorithms, databases), which are banal because they exist "largely beyond public discourse or contestation" (Goold, Loader, and Thumala 2013: 978). Due to their technical complexity and lack of public understanding, banality also entails the difficulties of identifying problematic elements in such systems, where the most visible part is often not the most problematic. Banality inoculates against public oversight, even if it is not a deliberate strategy to evade scrutiny by actors involved in infrastructuring. Third, ALPR systems are framed as having immediate positive ends by those who deploy them (e.g., reducing pollution or improving zoning control). However, banality also describes the inadvertent and unpredictable potential of function creep, the broadened use of a technology beyond its original goals, emerging from processes of infrastructuring in the long term.

The perspective of banal surveillance does not assume that ALPR and similar systems are unimportant, or that citizens are completely unaware of their potential dangers. Rather, banality draws attention to the gradual shaping of infrastructures into accepted ways of approaching social and political problems through technological solutions. This process includes commanding the complicity and tacit consent of surveilled subjects (Bellanova, De Hert, and Gutwirth 2010) while deferring the consequences of such infrastructuring to an indeterminate future. For this reason, rather than focusing on citizens' perception of ALPR or public debate around it, we focus here on the actors that develop and deploy these systems in Denmark.

We situate this study in the fields of critical algorithm studies and surveillance studies. Our methodological approach takes "algorithms as culture" (Seaver 2017): not as strict technical objects, but as integrated in social and institutional arrangements. Responding to calls by Seaver (2017), Dourish (2016), Kaufmann, Egbert, and Leese (2019), and Wieringa (2020) for context-specific investigations of algorithms, we empirically analyse how the infrastructural components in ALPR configurations are deployed and reflected upon by the actors who implement them in Denmark. We take Denmark as a specific context where a high level of digital public service provision (see European Commission 2020) goes along with strong legislative and regulatory oversight, not least concerning the EU-wide General Data Protection Regulation (GDPR). We find evidence that the deployment of such systems is replete with legal and technical obstacles, with the example of policing representing the most controversial case.

Each deployment of an ALPR system is a response to particular goals where the configuration is restrained by budgets, legal restrictions, and the definition of the problem "solved" by ALPR. The case study of ALPR in Denmark shows that there is not a straightforward connection between wide-ranging data capture or analysis and mass surveillance, especially since the legal, political, and economic motives for deploying ALPR systems as infrastructures tend to differ substantially. By showing the different technical setups in parking, environmental zoning, and policing, we aim to build up a critical awareness of its particular operations. This empirical approach serves to avoid what Lee Vinsel (2021) describes as "criti-hype": The inflation of hype around surveillance technologies by critical scholars. Such "wishful worries" around surveillance often overstate the efficiency of algorithms and the claims of actors who sell them.

To present ALPR as a banal infrastructure, we focus on two research questions:

> RQ 1) How are ALPR systems developed, implemented, and interpreted by private and public actors in Denmark for parking, policing, and environmental zoning?
>
> RQ 2) How is ALPR configured as a particularly infrastructural form of algorithmic surveillance, and with what consequences?

These questions have been approached through qualitative research methods, in particular digital ethnography (Markham 2017; Pink et al. 2016). We conducted eleven qualitative interviews with key actors working with ALPR systems in Denmark. These took place from June 2020 to May 2021 and included members of the Danish Police, parking companies, ALPR manufacturers/distributors, environmental regulators, activists, and journalists. Due to COVID-19, almost all of these interviews occurred through video calls, which were recorded and transcribed. The transcripts were supplemented with a fieldwork visit to a unit in the Danish Police and the collection and analysis of marketing/press releases, video presentations, and other relevant documentation (e.g., court cases, legislation). Throughout the text, the names of interviewees have been pseudonymized.

First, we offer a brief overview of the literature on algorithmic surveillance and ALPR. Second, we present how ALPR is infrastructured through different components and configurations. Third, we present our findings on the implementation of ALPR systems in Denmark across the domains of parking, environmental zoning, and policing. Fourth and last, we discuss how banal surveillance is an outcome of this process of infrastructuring, which in turn yields a high potential for function creep.

Literature Review

ALPR systems represent an overlooked instance of "dataveillance" (van Dijck 2014: 205) or simply a new form of "infrastructural surveillance" (Gekker and Hind 2020) by combining built infrastructure, camera technology, networking and data processing, storage, and analytics. The primary input for ALPR systems are the license plates of moving or still vehicles. The deployment of ALPR systems connects theoretically and analytically to two main strands of research in critical algorithm and surveillance studies.

ALPR as a Technology of Surveillance

ALPR systems rely on camera technologies and therefore stand in a historical line with what Daston and Gallison (2007: 17) have called objective images, photographic images that "[bear] no trace of the knower" because they are generated automatically. This kind of image represents a form of objectivity based on "blind sight, seeing without inference, interpretation, or intelligence" (Daston and Gallison 2010: 17; cf. Tagg 2009). The few articles that discuss ALPR highlight "the contemporary linkage of multiple data stores with automated image sensing technologies [enabling] a previously unheralded ability to massively surveil resident and transient populations" (Parsons et al. 2012: 2). Because ALPR technology is aimed at capturing license plates irrespective of concrete suspicion, it raises a number of "puzzles" for the protection of privacy (Warren et al. 2013). ALPR is similar to facial recognition technologies in that it automates the occurrence of a particular, predefined pattern into a machine-readable data point (Agre 2003; Goold, Loader, and Thumala 2013; Smith 2020). Yet, ALPR differs from traditional CCTV surveillance as it automatically turns particular, predefined details of recorded images (i.e., the license plates) into identifiable data that can be stored and subsequently analyzed. Cameras and data processing are part of a wider surveillant assemblage "providing for exponential increases in the degree of surveillance capacity" (Haggerty and Ericson 2000: 610). While we are sympathetic to the concept of surveillant assemblage, we will here speak of *configurations of components* to describe ALPR as a specific technology of surveillance.

ALPR systems are equally relevant for the study of algorithms and their variegated uses (Dourish 2016). By "automating vision" (McCosker and Wilken 2020) to capture the movements of cars, such systems create a plethora of what Amoore (2011: 28) calls "data derivatives," fostering the "emergence of novel forms of correlation" between previously unrelated events, entities, or processes based on computation. As such, they are relevant as political entities that shape how society is monitored, understood, and governed (Campolo and Crawford 2020). Based on an "abstraction of individuals into decontextualized encodings" (Leszczynski 2016: 1701), readings of license plates can be used for gathering intelligence on the movements of cars, enforcing regulations, administering fines, determining registration, or even training machine learning algorithms to identify predefined patterns (see O'Malley 2010 for further discussion on "telemetric policing").

ALPR and Policing

ALPR is regarded as a crucial technology especially for policing public spaces, which explains the increased amount of literature dedicated to this use case. Following the integration of real-time readings of license plates with existing data assets, ALPR systems can be regarded as "dragnet surveillance tools—they take readings on everyone [that passes by the camera], not just people under suspicion" (Brayne 2020, 2017). They are promoted to reduce costs, increase efficiency of police work, and improve criminal investigations (Ozer 2016; Benbouzid 2019). Through dragnet readings and processing of license plate data in real time, ALPR systems enable mass surveillance and purportedly "predictive policing" (Shapiro 2020). Real-time ALPR data can be used to support analytic models of crime patterns, to map spatial movements of lawbreakers, and as a source of information to officers on the street. As such, ALPR is lauded by Police Departments as an objective technology to justify and legitimize public spending on crime prevention and investigation (Karppi 2018).

But in criminological research, in everyday police work, and in surveillance studies more generally, the status of such predictive modelling based on past behaviors remains highly contested (Harcourt 2007; Jansen 2018; Meijer and Wessels 2019; Minocher and Randall 2020; Eterno, Silverman, and Berlin 2021). The main target of critique is the choice, weighting, and interpretation of data points feeding the models of police work because patterns "unfold considerable epistemological authority" (Kaufmann, Ebert, and Leese 2019: 684). They are politically relevant since they often "do not disclose the assumptions and decisions that inform the design of algorithms" (Kaufmann, Egbert, and Leese 2019: 684), posing significant problems to "algorithmic accountability" (Wieringa 2020) and the "politics of computation" (Ziewitz 2016: 4). These systems need to be comprehended as social not only in their production and weighting of data but also in their uses and effects and how these are all interconnected (Brayne 2021).

ALPR systems are relevant as infrastructural investments by the police or municipalities, aiming to capture vehicle movements in real time to integrate and compare with individual archived records, tax filings, or criminal data. Suppliers and users of ALPR systems in policing anticipate pre-emption of crimes as a possible outcome of such scopic data analysis and integration (Egbert and Krasmann 2020) that mobilizes a "rhetoric of imminence combined with the goal of automation" (Andrejevic 2017: 893) to mitigate future risks (cf. Andrejevic, Dencik, and Treré 2020). In sum, ALPR is discussed in policing because it carries particularly problematic possibilities for biased or unjust algorithmic decision-making, including the assumptions of prediction and pre-emption.

ALPR is a visual technology of surveillance that normalizes algorithmic vision and automated decision making. It is dominantly discussed in regards to the policing of public spaces. However, as we show, ALPR systems are also deployed in other contexts. This requires us to closely inspect their specific configurations and components.

Infrastructuring Automated License Plate Recognition

ALPR can be regarded as an extension of CCTV infrastructures that were implemented for traffic control and the surveillance of public spaces at least since the 1950s in different European countries (see Kammerer 2009). Dedicated experiments with ALPR go back to first deployments in 1984, when police scientists set up cameras with automated reading capabilities between London and Leeds. Since then, the UK has continued to be a central country for the use, development, and export of ALPR technologies (Bridle 2013).

ALPR's infrastructuring goes beyond the most visible part of its configuration: the camera next to a road. ALPR systems in Denmark and elsewhere generally include at least four common components: (1) a camera, (2) an algorithmic processing unit, (3) on-site/remote data storage, and (4) interfaces to different analytics solutions.

Camera

The camera units of ALPR systems can be affixed to walls or poles, or they can be located on mobile police or inspection cars. Their price range can vary widely, as the demand for resolution and accuracy differs between use cases. Sensors and resolution need to be attuned to the purpose, as capturing license plates from high-speed cars on highways poses different challenges than parking lots, where cars typically approach at low speeds. Cameras use infrared light for reading license plates, which is useful for identifying high contrast areas (i.e., between white background and letters) in adverse light conditions. In order to increase accuracy or coverage, cameras may also be deployed in a redundant fashion to confirm the accuracy of readings by comparing images from different angles or distances. A camera may also take more than twenty pictures of each passing car in order to algorithmically select the one that is most legible.

Algorithm

It is important to distinguish between the *capture* of images by cameras and the different algorithms used for the *recognition* of license plates (Lubna, Mufti, and Shah 2021: 2–3). ALPR systems require OCR (Optical Character Recognition) algorithms to transform captured images into machine-readable data points. Algorithms are first employed for different microtasks such as number plate extraction (from the larger image), character segmentation, and character recognition. The recognition of alphanumeric characters most often uses a rule-based algorithm, the most computationally efficient method. However, contemporary systems may also use a machine learning (ML) algorithm trained on a large-scale data set whenever the first model doesn't render accurate results. ML enables higher precision, but it is also more resource intensive.[2] The OCR algorithm may be located onboard the camera, on a server, or on "the cloud" (on-demand servers purchased from large corporations such as Microsoft or Amazon). The specific OCR algorithms used in an ALPR system are usually proprietary, with each vendor developing particular techniques that are fine-tuned for the regions in which they operate. Furthermore, images may be directly anonymized by blurring out parts of the image that are not license plates.

Storage and Databases

The resulting license plate readings are most often transferred through wired networks or mobile connectivity to a server or the cloud. Each stored reading is accompanied by metadata such as time, location, and (where applicable) speed value, the brand of the car, or other information extracted by algorithmic processing. Depending on the use case, readings may not be stored at all, or data may be fully anonymized. The specific configuration of what data are stored, how they are stored, and how they are processed or analyzed follows from the design requirements of clients as well as the resources available for system development and deployment. Storage and database usage may be deliberately kept small if the use case is narrowly defined.

[2] The basis for ALPR algorithms is, of course, the heavily standardized design of the license plate itself, which differs less between European Union member states than between states in the US (cf. Young, Katell, and Krafft 2019).

Analytics/Interface

Depending on the use of the ALPR system, recorded license plates are run through different forms of data analytics. License plate readings may be compared with information from databases of "whitelists" (i.e., authorized vehicles) or "blacklists/watch lists" (i.e., unauthorized or suspicious vehicles).[3] These may result in alerts, notifications, or new records in a database. These readings may also be cross-checked by human workers, especially if they need to be confirmed for legal reasons (such as the enforcement of fines). In the case of policing, this interface may mean an integration with Excel sheets of a car's movement that are analyzed by officers or Application Programming Interfaces that enable automatically sending an email alert whenever a suspected car passes by a camera. In the case of parking, interfaces may be constructed to display graphs showing parking lot occupancy for managers, customers, or other third-party service providers.

The infrastructuring of ALPR is realized through configurations of these main components that fulfill the goals of their envisioned use case. However, such configurations find their limits in the specifics of the installed hardware. For example, a camera installed in a parking lot does not operate as well on a road. Moreover, some systems are implemented by private companies, with different consequences for data integration and future use than would be required by the government or the police. Understanding the processual character of infrastructuring highlights that any change of components creates consequences for operators, and, as we will show in the case studies, implies restrictions on the potential for surveillance in each use case.

ALPR Deployment in Denmark: Parking, Environmental Zoning, and Policing

To better understand how configurations of ALPR readers, algorithmic models, and aspirations for data analysis matter in different contexts, we discuss three specific cases of the deployment of ALPR in Denmark. These contexts include: the use of ALPR to simplify parking fees; the control of environmental zoning regulation with a high degree of privacy protection; and the surveillance of roads by the Danish Police fighting "serious and organized crime." In each case, the configuration of ALPR differs, yet the potential for function creep from banal surveillance can be identified.

Parking: Seamless Charging for a "Barrier-Free" Customer Experience

ALPR is used by privately owned parking lots to create a more convenient customer experience.[4] In Denmark, the parking industry has long been associated with exorbitant fines and poor customer service. In the past few years, companies have begun experimenting with digital services to remedy this public perception (e.g., apps for registering and paying for parking such as EasyPark). Since 2016, there has been a push for fully automating parking fees. Instead of handing out paper stubs for payment, ALPR cameras are installed to register every car upon entrance and exit in lots. Customers are asked to pay either through a parking app or a pay-and-display machine. Such ALPR-equipped lots operate completely without barriers to entry and exit. They feature an infrastructure for a seamless "user journey," as Malthe, the director of a company that distributes ALPR equipment for parking, explains, "In my world, and in 2020, when you drive into a parking area, parking is never your primary goal. There's always something you have to do: visit a shopping center, cinema, restaurants, whatever. That's the primary goal. But parking is the first and the last thing you remember when you go to this restaurant or cinema. So it has to be as easy as possible." Interviewees in the industry pointed to convenience, comfort, and "easing the user journey" as their key motives for deploying ALPR systems for parking. The lack of physical barriers reduces congestion at the entry/exit points from public roads and makes the collection of fees from customers via dedicated apps more

[3] We acknowledge the racialized implications of "whitelisting" (as positive) and "blacklisting" (as negative) but use these terms here for the sake of consistency with industry terminology.

[4] In this section, we focus on the way privately owned parking companies use this technology. There are also examples of its use by cities (such as Copenhagen) for regulating public parking.

efficient and transparent. Since parking duration is registered automatically through ALPR systems, the technology also reduces the risk of people parking and not paying.

Although ALPR systems in parking lots are implemented to simplify parking, customers often have problems understanding how these systems work. Some customers simply forget to pay because they don't notice the camera, while others even forget their license plate numbers. As described by Emil, a manager in a parking company: "[F]rom our experience, it is still an issue for people not having a barrier. It's an issue that when they leave […][5] there's nothing physically stopping them from going out before they have paid, then a certain percentage will not pay […] not because they do not want to pay, but because they forget it, even though we put a gazillion signs." Automation thus creates a much greater need for customer service to handle diverse kinds of customer requests, including calls from people checking if they have paid correctly. If customers forget to pay, they have forty-eight to seventy-two hours to use the app to pay. If no payment is made, the parking company uses a third-party service to collect the payment alongside a service fee. The companies we interviewed indicated that this procedure was beneficial to customers, as the service fee is much lower than the fines given to car owners in the previous model.

But the deployment of ALPR systems also turns companies primarily managing parking lots into data-handling companies, with additional needs to communicate with customers and the wider public. This development adds new challenges to the business: managing data streams from ALPR systems securely while respecting the privacy of customers. As further explained by Emil, a manager in a parking company, "What people come to realize after digitizing stuff is that you actually need more people to handle all of the digital aspects of things. I mean, if you look at the Danish society, we are trying to digitize everything […] But you actually need humans, at least for now, to actually manage those systems. So the more you know, the more people you have to have to manage those systems." This points to the complications for lot operators emerging from having to manage the personalized data assets created by ALPR automation. A crucial consideration is the security of information systems used for processing ALPR data, including the lurking threat interviewees felt from GDPR regulation. Emil even mentioned that his company is "dialing [ALPR deployment] a bit back" because the Danish Data Protection Agency "is closing in," as the agency is increasingly regulating all forms of "mass data storage." Parking operators are thus, according to him, "forced to handle [personal data] with care and not just spread data around."

ALPR data for paid parking are usually kept for up to thirty days in order to respond to possible customer complaints. For unpaid parking, data are kept until customers have paid their fee. Such data retention periods are not directly dictated by GDPR or the Danish Data Protection Agency but reflect the companies' interpretations of the regulation for operative demands in their business. Before the regulation by GDPR, some parking lots used to check the recorded license plates in the national registry to see which postal code was associated with the car (which was the only publicly available information about vehicle registration). This allowed them to build a heat map of where customers came from in Denmark. With the new regulation, developers and users of ALPR systems for parking actually prefer only keeping anonymized records that serve for the analysis of peak occupancy times and seasonal patterns. Storing non-anonymized data beyond their original purpose creates legal liabilities, especially since businesses cannot use such data for other purposes. As described by Viktor, a product manager in a company that develops ALPR solutions, "[W]e would like to delete the data the second […] the car leaves […] you could argue there's some value for the customer [i.e., parking lot] if they could say: this license plate has entered four times this month. […] But we don't want to support this. We have actually decided internally that the way we want to approach data security is we want to store as little as we can."

The promise of ALPR automation for parking is built on a very standardized and rather banal social problem: automatically and seamlessly paying for parking. Technical functionality aside, it is evident that not all customers easily adapt to such systems, as many forget to pay or contact customer support with issues. The

[5] Throughout this article, we use bracketed ellipses to represent omitted text. Non-bracketed ellipses represent an interviewee's faltering or incomplete speech.

legal obligations imposed by GDPR and the need for securing customer data, in turn, introduce new obligations for parking lot operators. Such issues reflect how automation through ALPR finds limitations both in user practices and demands for legal data management. Although parking data could be used for extensive consumer surveillance, our case study shows that, in Denmark, legal regulation makes operators refrain from such practices (at least for now), with companies preferring to dispose of personal data as soon as payments for parking are made. Operators are pondering the possibilities of stronger integration of their parking data with customer benefit schemes and shopping mall loyalty cards, which could require amendments to the current data retention regulation.

Environmental Zoning: Enforcing Low Emission Zones through Automating Fines

Environmental zoning through ALPR systems is a policy measure that seeks to achieve a reduction of toxic emissions from traffic in downtown areas in Denmark. The administrative responsibility for this infrastructure rests with a national agency in Denmark. ALPR systems in this use case operate within a narrow political and legal mandate, reflected in the system configuration that aims to reconcile the public demand for clean air while protecting (to some degree) the privacy of citizens.

Environmental Zoning goes back to 2006, when "Low Emission Zones" (LEZ; in Danish, "Miljøzoner") were created to ban older, highly polluting vehicles (especially diesel trucks and vans) from entering highly populated city centers. In 2020, the Danish Environmental Protection Agency (Miljøstyrelsen) was given a political order to enhance the enforcement of this regulation. Sund & Bælt (S&B), a Danish state-owned company, was appointed to establish an ALPR solution for this purpose. A legal basis was approved by the Danish Parliament, appointing S&B for the project and setting explicit limitations for the use of the technology and the processing and retention of data. The choice of S&B occurred due to its previous experience with ALPR as part of the "pay-by-plate" tolling infrastructure on the country's bridges. In contrast to the toll collection system, the ALPR for enforcing low emission zones is used solely for fining infringing vehicles. Fixed ALPR cameras were installed in the four largest cities in the country (Copenhagen/Frederiksberg, Aalborg, Aarhus, and Odense), with fifteen different sites and a total of forty-three fixed cameras, some of them installed to monitor multiple lanes individually (as of July 2021). Additionally, five mobile ALPR units were purchased.

The political goal of ALPR in this case is reducing toxic emissions in cities to increase air quality. As the Mayor of Copenhagen, Lars Weiss, described to the media, "The aim of the law is to avoid old diesel cars inside the city that emit a lot of NOx gases and particles, because they are the ones that kill Copenhageners early" (qtd. in Nathan, Løkke, and Nørgaard 2020). Before the automation of environmental zoning through ALPR, police officers checked manually for polluting cars. Alongside other duties, the enforcement rate of this process was low. By contrast, ALPR operates continuously and cameras register license plates from every single passing car, irrespective of whether the vehicle is allowed into the city or not. Although there are only a few sites in each of the four cities, and potential offenders can circumvent roads with installed cameras, the increase in enforcement has been substantial, according to S&B. For example, local media reported that with the new system around five-hundred fines were handed out across two months of 2020 just in the city of Odense (Peter 2020).

Because ALPR systems capture all license plates of passing cars, specific design choices were made to safeguard the privacy of drivers. The ALPR system for environmental zoning operates on a "list-based enforcement model." This model reduces the amount of information logged because each camera receives, through a secure mobile internet connection, a list of cars that *are authorized* to enter the city. If one of these cars passes by the camera, and its license plate is correctly read by the algorithm running inside the camera, its presence is not recorded by the camera or transmitted to the company's server. The system is designed to actively track only cars that are *not allowed* to enter the city (i.e., polluting cars), foreign cars that have not yet been added to the database, or those whose license plates are not identified with a high degree of certainty. Positive readings or "hits" are transmitted to the company's server, where employees manually confirm the infraction and issue fines to the registered owner (a form of "telemetric governance," in the words of O'Malley 2010).

The list-based model was chosen due to the legal regulation of environmental zoning through ALPR, which itself was directly shaped by the requirements of the GDPR. The regulation stipulates that data from cars registered as nonpolluting should be deleted "within a few seconds." Sofie, a manager in S&B, goes as far as saying that the system has been developed to "try to see as little as possible," also pointing out that the camera itself blurs the face of the person driving the car. Therefore, the technical setup, data processing, and administrative procedures follow directly from the legal restraints imposed by legislation.

ALPR in environmental zoning is a technological solution to a social problem, normalizing banal surveillance for an ostensibly good purpose (i.e., reducing pollution). By championing a technology that checks every single passing vehicle, the legal grey zone of entering a city without permission is largely diminished in favor of a technically determined adjudication of legal/illegal behavior (see e.g., Kaufmann, Egbert, and Leese 2019). What was previously the professional judgement of a police officer to enforce a law or to choose not to is now deferred to a system automatically operating on determinate parameters of legality (see Wells 2008 for further discussion on such procedural forms of justice).

Yet, even in a system that seems to respect privacy to a high degree, the potential for function creep still exists. This form of infrastructuring also creates legitimacy for continuous and non-discriminate monitoring and surveillance of citizens, including new and problematic uses. Although not yet an immediate reality, there are signs that political demands could shift based on the existing infrastructure now in place. In January 2021, for example, a letter was sent from several influential organizations to the Minister of Justice, asking for police access to data from environmental zoning ALPR systems to fight the different problem of "social dumping," or the illegal use of immigrant labor (Nielsen et al. 2020). The Minister's response at first indicated that this possibility would be investigated (Hækkerup 2020), but when asked again, he ruled out this possibility indicating that the infrastructures of environmental zoning could not be integrated with those of policing (Hækkerup 2021). Such potential of function creep in banal surveillance underlines how infrastructural configurations and their legislative regulation are closely connected.

Policing: Widening Dragnet Data Collection with Little Public Oversight

The more problematic aspects of banal surveillance through ALPR systems become apparent when we look at the Danish police. ALPR was initially deployed as a border technology to combat "serious, organized and cross-border crime" (Politi n.d.). This initial goal, however, has prompted wider and more thorough ambitions to use ALPR for data-driven policing, investigation, and intelligence. Cameras across Denmark have increased, as has the retention period for data. But the benefits and costs of ALPR for policing remain complicated and questions about its actual efficacy remain unanswered.

Since 2016, ALPR cameras have been systematically deployed in Denmark to control border crossings. Such use of ALPR was justified by the Danish Parliament to mainly combat three forms of cross-border crime: (1) gang crimes, especially shootings and explosions; (2) terrorism (e.g., bomb attacks); and (3) Mobile Organised Crime Groups (MOCGs), defined as criminal groups quickly moving from country to country to commit property crimes or frauds. Since 2016, and due to strong political support, the ALPR's use has broadened beyond border control, with coverage increasing from 48 to 171 mobile cameras on top of police cars and 24 to 160 stationary cameras, most of which are placed at border crossings and large highway junctions. In 2022, the police expect a further expansion of the system to a total of 276 mobile and 272 stationary cameras, which will enable an even more granular analysis of vehicle movements across the country.

Based on our fieldwork at the Danish Police, there are at least three ways in which ALPR is currently used:

1. *Generating alerts for cars on a "watch list":* Notifications are sent to officers or investigators when, for example, a vehicle associated with an alleged gang member enters a certain region. Alerts also serve quotidian policing, particularly through mobile ALPR cameras on top of police cars (e.g., a dashboard warning if the owner of a passing car has not paid their insurance). Continuous and real-time

surveillance enables police officers to either react immediately or simply record the instance for future analysis.

2. *Investigating crimes by analyzing historical data sets of vehicle movement*: This includes using various interfaces to filter data of where a specific car has been over the past month (or longer) to generate new leads.
3. *Building intelligence through analyzing patterns:* This can include analyzing movement patterns of members of a particular gang, forecasting future crimes, and adopting preventive measures. Building intelligence from ALPR data requires the involvement of analysts with specific skills for modeling, data integration, and pattern recognition.

As can be seen in these use cases, the ALPR system serves a much wider function than just "serious and organized crime." In reality, it operates within the wider goal of turning the police into a data-driven organization, part of a push for "Intelligence-Led Policing" (ILP). Originating from the UK, ILP proposes that instead of a "reactive policing" model where police just respond to incidents, evidentiary information should be collected and analyzed continuously (and preferably beforehand) to inform police action and predict or prevent crime in an objective manner (Kaltoft 2020). ALPR is seen as a key strategy in generating data for such a goal, especially as it is based on purportedly efficient and automated surveillance.

In order to produce such intelligence, ALPR depends on "dragnet" data collection. It gathers information from all cars that pass by the cameras and stores this information on police servers. Although a lot of data are collected, almost none of them are actually used, and very few of the readings are actual "hits," i.e., cars that are on the "watch list" (cf. EFF's analysis of ALPR in California in Maass 2021). Still, both the Danish Police and the Danish Minister of Justice have sought to extend the period for which data can be kept. Originally, "no-hits" could be kept for only twenty-four hours to comply with the ALPR regulation in the country (Justitsministeriet 2017). However, the regulation also indicates that an extension to thirty days is permitted in the case of a time-limited and geographically targeted operation. For many years, due to this exception, the Danish Police have considered almost all of the country a "targeted operation" and thus increased data retention periods. Just in a month of 2018, for example, over twenty-one million captures of license plates became data points in the "no-hit" database (Hækkerup 2018). Now, in 2021, the Ministry of Justice is seeking to officially extend the retention period to sixty days, with the justification of supporting the investigations of past cases.

The expanding use of ALPR surveillance is highly praised by Danish politicians and police representatives, but the obstacles to its efficient deployment are considerable. Interviewees in the police pointed out that the ALPR system offers a lot of information about the movement of vehicles, but additional information and sources are always needed for making sense of data for investigations and intelligence. As described by Nick, a senior manager in the Danish Police:

> We get a lot of data out of ALPR. But it's difficult to say what the data is actually telling us… because it's like…. there's a lot about cars [but] I don't know who's driving them. […] I need to have a needle first, I need to have something that's saying to us: this guy, or these cars, are suspicious. When I have that, and I have the data set, it makes a huge difference. And we can find people who are running away from the police… […] we have found a lot of stuff when we have the data set.

As described by Nick, ALPR data are little more than the readings of license plates. In order to make this data useful for investigations or intelligence, it requires cross-referencing with other public or internal data sets, as well as old-fashioned police investigation. The metaphor of the "needle in the haystack" used by Nick and other interviewees aptly describes the difficult human labor of filtering the immense volume of data for useful leads.

The quality of ALPR data is also a concern. Although companies promise 99.9% accuracy of read rates from cameras, these numbers have not been publicly audited by external organizations or even by the Danish Police. Errors can occur for different reasons, such as adverse environmental conditions. Cameras on fixed poles also have better read rates than vehicle-mounted units due to capture conditions. As a consequence, the data quality of ALPR is subject to much uncertainty, requiring critical self-reflection from investigators to avoid errors. While systems like the Danish CPR (Civil Registration Number) are regarded as containing precise information about a citizen's address and name, ALPR is regarded to be questionable. As Nick points out in the following exchange:

> Nick: So this is where we really need to be aware as analysis workers, is to be so critical about the data set. […] when I look at the ALPR system, it puts out a hit list, I can see the hits. Yes, I get 100%, it feels like I get 100% of data.
>
> Interviewer: But you're not?
>
> Nick: I don't think so. No, I'm not… for sure I'm not… But what if I only get 50%?

ALPR is lauded as a "fundamental tool for fighting crime" because its automated and data-driven qualities are perceived as neutral and effective. However, its actual operation is largely left unquestioned, even though no one knows exactly how effective it is. The dragnet it enables, though it comes at the cost of much labor and plenty of limitations, continues to grow. The reason for that resides precisely in its character as a "technological fix," as indicated by Nick:

> The ALPR system is growing fast. Very fast. I think for different reasons. And one of the reasons is that it's easy to understand, and that it's easy to invest in. It's like:
>
> [pretending to be talking to a superior]
>
> "So, what do we need?"
>
> "I need well trained and well-educated people [officers.]"
>
> "Oh, I don't know how to fix that… [pause]. Oh, so you need like 100 cameras."
>
> "Yes."
>
> "I can write you a cheque right now and you'll go and buy."
>
> So that's… there's some of it that is a quick fix.

The growth of ALPR in the Danish Police is part of a wider push to expand surveillance by automation and digitalization, exploiting the alleged objectivity of ALPR. Much like in other countries, such as the UK (Bridle 2013), the surveillance network continues to grow without much oversight or public participation (cf. Young, Katell, and Krafft 2019). The automation of detection and tracking provided by ALPR presents itself as efficient and all-seeing, but as shown by the limitations and concerns raised by officers, this is far from a reality. The Danish Police keep data for longer periods and use it for various purposes, often without defining these purposes at the outset. There is a persistent threat that, without informed public oversight and transparent governance, such dragnet surveillance may grow even further and be used in particularly harmful ways. The use of ALPR is based on similar infrastructural components as previous cases. Yet, the broad interpretation of legal constraints by the Danish Police, as well as the amount and granularity of data, yields the biggest potential for function creep and biased/unjust analysis. These need to be understood alongside the other biases of police investigative work, which predate ALPR systems.

Discussion: From Banal Surveillance to Function Creep

Throughout the three cases, we describe how ALPR operates as a form of banal surveillance, as these systems become infrastructural forms of algorithmic data capture and analysis. ALPR normalizes the acceptance of surveillance for politically and socially desired purposes (parking, environmental zoning, policing), even if its actual implementation is far from efficient or guided by minimal public oversight. In the discussion section, we want to raise a few concerns that make banal surveillance through ALPR systems particularly problematic and connect these concerns to wider debates in critical algorithm and surveillance studies.

Contrary to what may be assumed, the banal surveillance enacted by ALPR is far from an all-seeing algorithmic surveillance. These systems, as we have described them across the cases, vary depending on their configuration and goals, facing different issues of efficiency and functionality, legal restraints, and competences for working with data. Interpreting ALPR as a well-functioning surveillance system across different domains without understanding the details of its limitations, including a lower accuracy of read rates than is often acknowledged, would be taking at face value the imaginary of ALPR manufacturers and the police. In this respect, building off of Agre (2003), algorithmic surveillance works "well enough to be dangerous, and poorly enough to be dangerous as well." Either way, it is necessary to assess the situated deployment of particular infrastructural configurations before wielding the critical sledgehammer.

While based on continuous and concealed surveillance, ALPR systems *can* work in ways that refrain from recording and analyzing data from all people and their vehicles. Interviewees repeatedly referred to data they collect as potential "toxic assets" that need to be contained proactively (cf. Thylstrup 2019). Although they believe their systems are protected against abuse, all actors were aware that mass data collection through ALPR could potentially be harmful. They referred to GDPR as offering practical guidance on how personal data shall be protected but also pointed to new applications of ALPR that are not yet legally defined. For parking managers, the clear goal was to charge for parking efficiently, deleting data about clients as soon as their payment is received. The case of environmental zoning, then, shows how a system can be engineered to *not* store data from all passing cars. Although police intentionally use the system for mass (dragnet) surveillance, interviewees also mentioned their concern about respecting citizens' rights. These cases show how current regulation, including the GDPR, and actors' own ethical concerns negotiate between the demand of banal surveillance and the danger of mass surveillance.

The banality of ALPR systems is in part based on their acceptance and perception of positive functionality (e.g., seamless parking). Banal surveillance relies on the obscurity of what and how data are collected and analyzed, residing in a grey zone of regulation and public oversight. As components of ALPR systems change and data are integrated, new goals may be defined. This can lead to functions being performed beyond their initial goals, e.g., when data assets become inputs for more advanced analytics that weren't necessarily available when the system was initially implemented. This is the case of Environmental Zoning, as described above, where ALPR data are being enlisted in the fight against "social dumping." Regulation and actors' ethical concerns can also wane over time, especially as the system fades into the fabric of everyday life. The use of ALPR in policing is particularly worrying, as the recent expansion of sites of capture and periods of data retention have led to possibilities of analyzing vehicle movements at far more granular levels.

Such function creep is particularly problematic as contemporary ALPR algorithms can do much more than recognize only license plates. Systems now also reach higher accuracy in capturing vehicle brand/model and color. New algorithms can offer additional functionalities, such as occupancy analysis (how many people are in the car) or supplementing license plate data with facial recognition, although none of the companies we spoke with promoted this latter use. An example of function creep in ALPR is how the US company Vigilant Solutions enables "platform policing" by giving free ALPR cameras to police organizations while getting paid through fees added to the debt collection machines operated by officers (Linder 2019). Such forms of function creep that "[entangle] police and business to a novel degree" (Linder

2019: 80) cannot be seen in Denmark (yet), but the widening of the police ALPR dragnet is occurring at a rapid pace, including the connection with other data sources (cf. US "fusion centers" in Brayne 2017; see also the case of Flock Safety described in Holder and Akinnibi 2021).

The potential for function creep in banal surveillance technologies such as ALPR brings up the importance of visibility. To enable public oversight, citizens need to comprehend the potential of banal surveillance technologies beyond just cameras on the side of the road or the hype created by technology companies. It is important to make these cameras visible in their infrastructural dimensions: cameras that are connected to networks and linked to databases and analytical tools. Activists in Denmark have for the past years worked on a crowdsourced map (anpg.dk) of ALPR systems, which helps to visualize their expansion by the police and environmental regulators (Figure 1). However, it is not a legal requirement that police and the Environmental Agency communicate the positions of such cameras or how they operate. In reality, activists had to file many Freedom of Information requests to obtain the necessary information and construct their database, with information being selectively redacted by the police. Similar to the UK (Bridle 2013), banality also includes the deliberate or intentional hiding of surveillance, keeping devices out of sight or making it difficult to obtain information about such public infrastructures. As can be seen in the actions of these activists, "acts of vigilance" (Smith and O'Malley 2017) by citizens are a possible and indeed effective mode of resistance, as they can make visible these otherwise banal forms of surveillance. These forms of "crowdsourced countersurveillance" (Wood and Thompson 2018) and other forms of antagonisms to ALPR are topics we hope will be further addressed by future studies (cf. the discussion of "Infrastructural Investigations" in Dijstelbloem 2021).

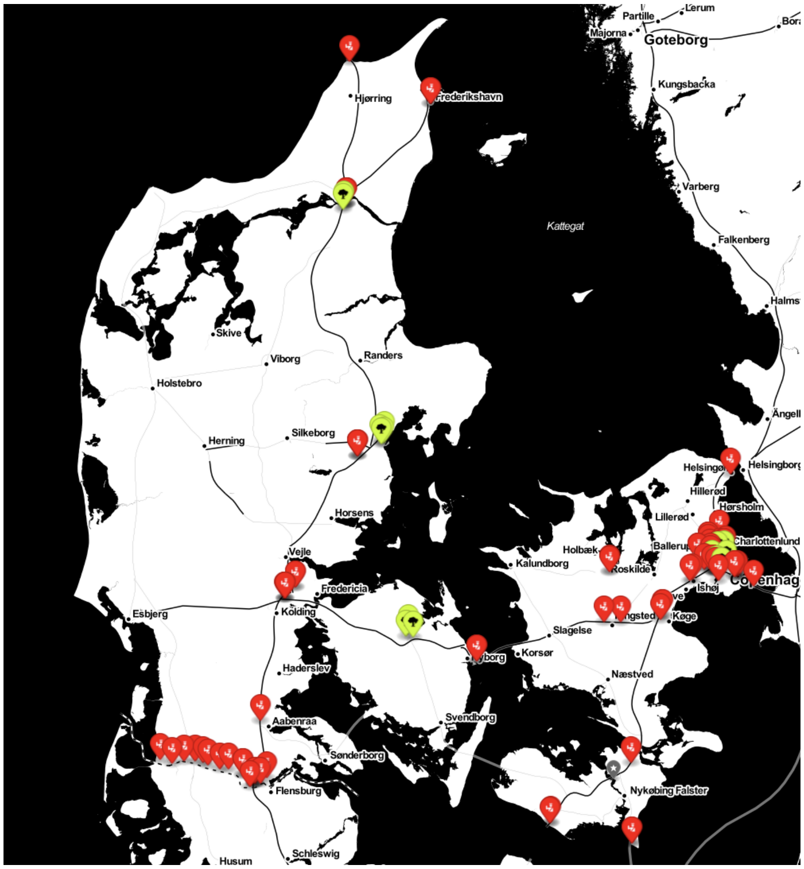

Figure 1: *Screenshot of the crowdsourced map of ALPR in Denmark (**anpg.dk**) created by activists. In red, the location of stationary police ALPR cameras. In green, the location of stationary environmental zoning cameras. The map gets continuously updated as activists get information on new locations.*

Finally, infrastructuring for banal surveillance entails an unavoidable potential for function creep as data-driven governance yields new fields of application for the capture of personal data, integrated analytics, and even prediction. What then are possible safeguards against abuses? Once surveillance infrastructures are installed, they become very difficult to change or abolish. Forecasting critical repercussions for public freedom and liberties is especially important in the early stages of adoption when decisions of infrastructural importance are made. This forecasting needs to be embedded through new kinds of governance that include the perspectives of multiple stakeholders and must include the mandate to ban or prohibit potentially harmful uses of new technologies. In addition to forecasting, continuous public monitoring is needed, particularly when new technologies and use cases emerge. The Seattle Surveillance Ordinance (Young, Katell, and Krafft 2019; Lee 2021) is a case in point, showing how democratic participation can be involved in the process by providing information about systems and offering policy recommendations for their adoption or rejection. Moreover, this ordinance imposes continuous audits of such systems, which offer both oversight of their use and recommendations for changes (Alderson, Sumitani, and Jones 2020).

Conclusion

Our goal in this article was to bring nuance into how ALPR systems are deployed through empirically engaging with three cases in Denmark. We contribute to emerging discussions in critical algorithm and surveillance studies on the adoption of algorithmic automation in everyday life. Through the notion of banal surveillance, we describe the infrastructuring of algorithmic data capture and analysis occurring under the radar with uncertain consequences. As Kammerer (2009: 47) argues, "Any new media technology carries a persuasive force with it that is inversely proportional to the degree in which individuals have adopted a knowledge about the technology themselves." The case of ALPR is emblematic of how visibility and, consequently, public comprehension and oversight are needed to avoid these technologies fading into the comfortable infrastructural fabric and their potential expansion to more problematic uses (function creep). It is important to reassert that it is not inevitable for these systems to operate in a mass surveillant manner: design principles, use cases, actors, and regulatory guidelines can shape their features and operations to reduce their potential for misuse. However, it is also important to consider when and how citizens should have the democratic voice to reject the deployment of banal surveillance.

Acknowledgments

The authors wish to thank all interviewees for their crucial contribution to this research. Special thanks to the reviewers and editors for their helpful comments and suggestions in shaping this article.

References

Agre, Phil. 2003. Your Face Is Not a Bar Code. UCLA. https://pages.gseis.ucla.edu/faculty/agre/bar-code.html.

Alderson, Melissa, Megumi Sumitani, and David G. Jones. 2020. Surveillance Usage Review: Seattle Department of Transportation License Plate Readers. Seattle Office of City Auditor. http://clerk.seattle.gov/~CFS/CF_321882.pdf.

Amoore, Louise. 2011. Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society* 28 (6): 24–43.

Andrejevic, Mark. 2017. To Preempt a Thief. *International Journal of Communication* 11: 879–896.

Andrejevic, Mark, Lina Dencik, and Emiliano Treré. 2020. From Pre-Emption to Slowness: Assessing the Contrasting Temporalities of Data-Driven Predictive Policing. *New Media & Society* 22 (9): 1528–1544.

Bellanova, Rocco, Paul De Hert, and Serge Gutwirth. 2010. Variations Sur Le Thème De La Banalisation De La Surveillance. *Mouvements* 62 (2): 46–54.

Benbouzid, Bile. 2019. To Predict and to Manage: Predictive Policing in the United States. *Big Data & Society* 6 (1): 1–13.

Brayne, Sarah. 2017. Big Data Surveillance: The Case of Policing. *American Sociological Review* 82 (5): 977–1008.

———. 2020. Enter the Dragnet. *Logic Mag* 12. https://logicmag.io/commons/enter-the-dragnet/ [accessed July 12, 2021].

———. 2021. *Predict and Surveil: Data, Discretion, and the Future of Policing.* New York: Oxford University Press.

Campolo, Alexander, and Kate Crawford. 2020. Enchanted Determinism: Power without Responsibility in Artificial Intelligence. *Engaging STS* 6: 1–19.

Daston, Lorraine, and Peter Galison. 2007. *Objectivity*. Cambridge, UK: Zone Books.

Dijck, José van. 2014. Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197–208.

Dijstelbloem, Huub. 2021. *Borders as Infrastructure: The Technopolitics of Border Control*. Cambridge, MA: MIT Press.

Dourish, Paul. 2016. Algorithms and Their Others: Algorithmic Culture in Context. *Big Data & Society* 3 (2): 1–11.

Egbert, Simon, and Susanne Krasmann. 2020. Predictive Policing: Not Yet, But Soon Preemptive. *Policing and Society* 30 (8): 905–919.

Eterno, John A., Eli B. Silverman, and Michael M. Berlin. 2021. Police Leadership of Tomorrow: Comprehensive Compstat Performance Management Moving From Stagnation to Innovation. *Police Practice and Research* 22 (1): 886–902.

European Commission. 2020. Digital Economy and Society Index (DESI) 2020. https://digital-strategy.ec.europa.eu/en/policies/desi [accessed July 12, 2021].

Gane, Mike, ed. 1993. *Baudrillard Live: Selected Interviews*. London: Routledge.

Gekker, Alex, and Sam Hind. 2020. Infrastructural Surveillance. *New Media & Society* 22 (8): 1414–1436.

Goold, Benjamin, Ian Loader, and Angélica Thumala. 2013. The Banality of Security: The Curious Case of Surveillance Cameras. *British Journal of Criminology* 53 (6): 977–996.

Hækkerup, Nick. 2018. REU, Alm.Del - Spørgsmål Nr. 756. Justitsministeriet. https://www.ft.dk/samling/20171/almdel/reu/spm/756/svar/1512347/1942051/index.htm [accessed August 15, 2022].

———. 2020. Transportudvalget (TRU) Alm. Del – Spørgsmål 138. Justitsministeriet. https://www.ft.dk/samling/20201/almdel/tru/spm/138/svar/1734648/2316764/index.htm [accessed August 15, 2022].

———. 2021. Transportudvalget (TRU) Alm. Del – Spørgsmål 481. Justitsministeriet. https://www.ft.dk/samling/20201/almdel/tru/spm/481/svar/1788760/2406006/index.htm [accessed August 15, 2022].

Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–622.

Harcourt, Bernard E. 2007. *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. Chicago, IL: University of Chicago Press.

Holder, Sarah, and Fola Akinnibi. 2021. Suburbs of Surveillance. *Bloomberg*, August 4. https://www.bloomberg.com/news/features/2021-08-04/surveillance-startup-brings-police-tech-to-neighborhoods [accessed August 15, 2022].

Jansen, Fieke. 2018. *Data Driven Policing in the Context of Europe*. Data Justice Project, May 07. https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf.

Justitsministeriet. 2017. *Bekendtgørelse Om Politiets Anvendelse Af Automatisk Nummerpladegenkendelse (ANPG)*. Vol. BEK nr 1080 af 20/09/2017. https://www.retsinformation.dk/eli/lta/2017/1080 [accessed August 15, 2022].

Kaltoft, Anna. 2020. Intelligence-Led Policing and Digital Technologies: An ANT Investigation into the Analytical Knowledge Production of the Danish Police. MA Thesis, Copenhagen Business School. https://research-api.cbs.dk/ws/portalfiles/portal/62181021/844869_ILP_digital_technologies_final.pdf.

Kammerer, Dietmar. 2009. Police Use of Public Video Surveillance in Germany From 1956: Management of Traffic, Repression of Flows, Persuasion of Offenders. *Surveillance & Society* 6 (1): 43–47.

Karppi, Tero. 2018. "The Computer Said So": On the Ethics, Effectiveness, and Cultural Techniques of Predictive Policing. *Social Media + Society* 4 (2): 1–9.

Kaufmann, Mareile, Simon Egbert, and Matthias Leese. 2019. Predictive Policing and the Politics of Patterns. *The British Journal of Criminology* 59 (3): 674–692.

Kaun, Anne. 2021. Suing the Algorithm: The Mundanization of Automated Decision-Making in Public Services Through Litigation. *Information, Communication & Society*: https://doi.org/10.1080/1369118X.2021.1924827.

Lee, Jennifer. 2021. Creating Community-Centered Tech Policy. In *Affecting Technologies, Machining Intelligences*, edited by Dalida Maria Benfield, Bruno Moreschi, Gabriel Pereira, and Katherine Ye. Center for Arts, Design, and Social Research. https://book.affecting-technologies.org/creating-community-centered-tech-policy/.

Leszczynski, Agnieszka. 2016. Speculative Futures: Cities, Data, and Governance beyond Smart Urbanism. *Environment and Planning A: Economy and Space* 48 (9): 1691–1708.

Linder, Thomas. 2019. Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service. *Surveillance & Society* 17 (1/2): 76–82.

Lubna, Naveed Mufti, and Syed Afaq Ali Shah. 2021. Automatic Number Plate Recognition:A Detailed Survey of Relevant Algorithms. *Sensors* 21 (9): 1–35.

Maass, Dave. 2021. Data Driven 2: California Dragnet—New Data Set Shows Scale of Vehicle Surveillance in the Golden State. Electronic Frontier Foundation, April 22. https://www.eff.org/deeplinks/2021/04/data-driven-2-california-dragnet-new-dataset-shows-scale-vehicle-surveillance [accessed August 15, 2022].

Markham, Annette N. 2017. Ethnography in the Digital Era: From Fields to Flow, Descriptions to Interventions. In *The Sage Handbook of Qualitative Research*, edited by Norman K Denzin, 650–668. Thousand Oaks, CA: Sage.

McCosker, Anthony, and Rowan Wilken. 2020. *Automating Vision*. London: Routledge.

Meijer, Albert, and Martijn Wessels. 2019. Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration* 42 (12): 1031–1039.

Minocher, Xerxes, and Caelyn Randall. 2020. Predictable Policing: New Technology, Old Bias, and Future Resistance in Big Data Surveillance. *Convergence: The International Journal of Research into New Media Technologies* 26 (5–6): 1108–1124

Nathan, Ida, Regitze Løkke, and Malte Nørgaard. 2020. Amdi måtte købe ny bil: Miljøzoner har allerede kostet 4.536 bilister en bøde. *DR*, November 25. https://www.dr.dk/nyheder/regionale/hovedstadsomraadet/amdi-maatte-koebe-ny-bil-miljoezoner-har-allerede-kostet-4536 [accessed August 15 ,2022].

Nielsen, Michael, Jørn Hedengran, Rune Noack, Jesper Højte Stenbæk, Erik Østergaard, Lars William Wesch, Henriette Kjær, Allan Jensen, Kirsten Bork, and Jesper Kronborg. 2020. Anvendelse Af Nummerpladescannere Til Udvælgelse Af Objekter

Til Kontrol Af Kravene i § 8 c Og 8 d Lov Om Udstationering. Folketinget. https://www.ft.dk/samling/20201/almdel/TRU/bilag/83/2304693.pdf [accessed August 15, 2022].

O'Malley, Pat. 2010. Simulated Justice: Risk, Money and Telemetric Policing. *The British Journal of Criminology* 50 (5): 795–807.

Ozer, Murat. 2016. Automatic Licence Plate Reader (ALPR) Technology: Is ALPR a Smart Choice in Policing? *The Police Journal* 89 (2): 117–132.

Parsons, Christopher, Joseph Savirimuthu, Rob Wipond, and Kevin McArthur. 2012. ANPR: Code and Rhetorics of Compliance. *European Journal of Law and Technology* 3 (3): https://ejlt.org/index.php/ejlt/article/view/164.

Peter, Bergman. 2020. Miljøzone: Bøder på over en million kroner uddelt til vare- og lastbiler. *TV2 Fyn*, November 26. https://www.tv2fyn.dk/odense/miljoezone-boeder-paa-over-en-million-kroner-uddelt-til-vare-og-lastbiler [accessed August 15, 2022].

Pink, Sarah, Heather A. Horst, John Postill, Larissa Hjorth, Tania Lewis, and Jo Tacchi, eds. 2016. *Digital Ethnography: Principles and Practice*. Los Angeles, CA: SAGE.

Politi. N.d. Automatisk Nummerpladegenkendelse. https://politi.dk/faerdsel/politiets-faerdselskontroller/automatisk-nummerpladegenkendelse [accessed July 11, 2021].

Raetzsch, Christoph, Gabriel Pereira, Lasse S. Vestergaard, and Martin Brynskov. 2019. Weaving Seams with Data: Conceptualizing City APIs as Elements of Infrastructures. *Big Data & Society* 6 (1): 1–14.

Seaver, Nick. 2017. Algorithms as Culture: Some Tactics for the Ethnography of Algorithmic Systems. *Big Data & Society* 4 (2): 1–12.

Selinger, Evan, and Woodrow Hartzog. 2019. The Inconsentability of Facial Surveillance. *Loyola Law Review* 66 (101): 101–122.

Shapiro, Aaron. 2020. *Design, Control, Predict: Logistical Governance in the Smart City*. Minneapolis, MN: University of Minnesota Press.

Smith, Gavin J.D. 2020. The Politics of Algorithmic Governance in the Black Box City. *Big Data & Society* 7 (2): 1–9.

Smith, Gavin J.D., and Pat O'Malley. 2017. Driving Politics: Data-Driven Governance and Resistance. *The British Journal of Criminology* 57 (2): 275–298.

Star, Susan Leigh. 1999. The Ethnography of Infrastructure. *American Behavioral Scientist* 43 (3): 377–391.

Star, Susan Leigh, and Karen Ruhleder. 1996. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research* 7 (1): 111–134.

Tagg, John. 2009. *The Disciplinary Frame: Photographic Truths and the Capture of Meaning*. Minneapolis, MN: University of Minnesota Press.

Thylstrup, Nanna Bonde. 2019. Data Out of Place: Toxic Traces and the Politics of Recycling. *Big Data & Society* 6 (2): 1–9.

Vinsel, Lee. 2021. You're Doing It Wrong: Notes on Criticism and Technology Hype. *Medium*, February 1. https://sts-news.medium.com/youre-doing-it-wrong-notes-on-criticism-and-technology-hype-18b08b4307e5 [accessed June 10, 2021].

Warren, Ian, Randy Lippert, Kevin Walby, and Darren Palmer. 2013. When the Profile Becomes the Population: Examining Privacy Governance and Road Traffic Surveillance in Canada and Australia. *Current Issues in Criminal Justice* 25 (2): 565–584.

Wells, Helen. 2008. The Techno-Fix Versus The Fair Cop: Procedural (In)Justice and Automated Speed Limit Enforcement. *British Journal of Criminology* 48 (6): 798–817.

Wieringa, Maranke. 2020. What to Account for When Accounting for Algorithms: A Systematic Literature Review on Algorithmic Accountability. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, *Barcelona, Spain, January 27–30*, 1–18. New York: Association for Computing Machinery.

Wood, Mark Andrew, and Chrissy Thompson. 2018. Crowdsourced Countersurveillance: A Countersurveillant Assemblage? *Surveillance & Society* 16 (1): 20–38.

Young, Meg, Michael Katell, and P. M. Krafft. 2019. Municipal Surveillance Regulation and Algorithmic Accountability. *Big Data & Society* 6 (2): 1–14.

Ziewitz, Malte. 2016. Governing Algorithms: Myth, Mess, and Methods. *Science, Technology, & Human Values* 41 (1): 3–16.