sustainability

MDPI

Article

Ethical AI for Automated Bus Lane Enforcement

Caitriona Lannon [1], John Nelson [2] and Martin Cunneen [1,*]

[1] Accounting and Finance Department, Kemmy Business School, University of Limerick, V94 T9PX Limerick, Ireland; Caitiona.Lannon@ul.ie
[2] Department of Electronic & Computer Engineering, University of Limerick, V94 T9PX Limerick, Ireland; john.nelson@ul.ie
* Correspondence: martin.cunneen@ul.ie

Abstract: There is an explosion of camera surveillance in our cities today. As a result, the risks of privacy infringement and erosion are growing, as is the need for ethical solutions to minimise the risks. This research aims to frame the challenges and ethics of using data surveillance technologies in a qualitative social context. A use case is presented which examines the ethical data required to automatically enforce bus lanes using camera surveillance and proposes ways of minimising the risks of privacy infringement and erosion in that scenario. What we seek to illustrate is that there is a challenge in using technologies in positive, socially responsible ways. To do that, we have to better understand the use case and not just the present, but also the downstream risks, and the downstream ethical questions. There is a gap in the literature in this aspect as well as a gap in the actual thinking of researchers in terms of understanding and responding to it. A literature review and detailed risk analysis of automated bus lane enforcement is conducted. Based on this, an ethical design framework is proposed and applied to the use case. Several potential solutions are created and described. The final chosen solution may also be broadly applicable to other use cases. We show how it is possible to provide an ethical AI solution for detecting infringements that incorporates privacy-by-design principles, while being fair to potential transgressors. By introducing positive, pragmatic and adaptable methods to support and uphold privacy, we support access to innovation that can help us mitigate current emerging risks.

Keywords: privacy; camera surveillance; ethical risk; bus lane enforcement; ethical AI

Citation: Lannon, C.; Nelson, J.; Cunneen, M. Ethical AI for Automated Bus Lane Enforcement. *Sustainability* **2021**, *13*, 11579. https://doi.org/10.3390/su132111579

Academic Editors: Efthimios Bothos, Panagiotis Georgakis, Babis Magoutas and Michiel de Bok

Received: 16 September 2021
Accepted: 8 October 2021
Published: 20 October 2021

1. Introduction

This paper explores the challenges and ethics of using data surveillance technologies in social contexts. We present a use case that employs surveillance technology to provide a socially beneficial and environmentally positive outcome. In deriving a social benefit, however, we further erode privacy and the human right to privacy. In our use case, we've offered a means of narrowing or reducing the risks of privacy infringement and erosion.

What we seek to illustrate is that there is a challenge to using technologies in positive and socially responsible ways. To alleviate risk, we have to better understand the use case and not only the 'present' risks but also the downstream risks, and the downstream ethical questions. Not only is there a gap in the literature in this aspect, there is also a gap in the actual thinking of researchers in terms of understanding and responding to it.

Our use case is based in Dublin, where there is a plan to reduce road congestion by widening roads in order to build more bus lanes. Supporters of the plan point out that it will encourage a modal shift from cars to public transport, reducing emissions and increasing bus reliability. Detractors to the plan highlight impacts to trees, protected curtilage, communities and private front gardens. In addition, the land use will include more road space and additional lanes for traffic. Crucially, there are also doubts that the plan

may work. Existing bus lanes in Dublin are manually enforced with a history of violations and ineffectiveness. There is no plan to introduce automatic enforcement for the new bus lanes. This brings the effectiveness of any new bus lanes into question.

An alternative approach could be to use technology to improve bus reliability instead of widening roads. Many international bus priority schemes have improved the performance of existing bus lanes through solutions such as automated camera enforcement. By doing so, we aim to build a less burdensome use of roads. This could help mitigate more destructive impacts upon urban pathways.

Hence, we investigate how the application of ethical AI can create alternative ways to enforce bus lanes, thus alleviating traffic congestion in cities. We are then confronted with a scenario where to achieve the noted benefit, we introduce a new risk — that of privacy erosion. To mitigate and manage that risk, we propose technological solutions, which support the overall risk mitigation of social good. By introducing positive pragmatic adaptable methods to support and uphold privacy, we also support access to innovation that can help us mitigate current emerging risks.

A literature review and detailed risk analysis of automated bus lane enforcement is conducted. Based on this, an ethical design framework for this use case is proposed and potential solutions are described.

2. Literature Review

AI is revolutionising the lives of everyone, and it is crucial that it does so in the right way. While ethical use of AI fosters human creativity and potential, underuse of AI engenders opportunity cost and overuse or misuse generates risk [1]. Ideally, AI technology would be used ethically, in a way that maximises benefits and opportunities, protects privacy and mitigates additional risk.

This section addresses the values, benefits and privacy trends and risks associated with automated bus lane enforcement and also examines a selection of camera enforcement use cases around the globe. In this way, we are able to identify ethical risk mitigation practices, which can be applied to automated bus lane enforcement in order to maximise benefits and opportunities, facilitate privacy-by-design and avoid unintended consequences.

2.1. Values

The principlism system of ethics uses four moral principles to guide moral reasoning: autonomy, beneficence, nonmaleficence and justice [2,3]. These principles are inspired by bioethics and described by Beauchamp and Childress [2,3]. Floridi et al. (2018) suggest an additional fifth principle of explicability [1].

Autonomy is a basic freedom at the heart of humanity, which respects individual decision making. It includes positive and negative duty. Examples of positive duty in bus lanes include giving road users timely and clear information allowing them to make their own decisions, such as taking a different route. The second aspect of autonomy, negative duty, guides what authorities must not do, such as the selling of personal data obtained by CCTV cameras to third parties — which is suspected of happening with City Brain in China [4]. Since data commodification can offer a perpetual source of income for private companies [5], this consequence is inevitable with no regulations. Such a breach is potentially worse if facial recognition software is employed. The social costs of implementing facial recognition systems are not well understood because the methods involved in their design are opaque [6].

Beneficence means doing more than the minimum and promoting well-being for the benefit of humanity [1]. It also includes removing possible harms or risks. Camera enforcement along bus lanes promotes good in many ways, including increasing

inclusiveness by improving public transport and helping to reduce emissions. However, balancing risks and using a privacy-by-design approach is necessary to ensure well-being is sustained rather than depleted. A lack of enforcement or insufficient enforcement can reduce beneficence as the public good is then reduced.

Nonmaleficence means avoiding doing anything which is unjustifiably harmful [1]. An example of contravening this principle is failing to put cybersecurity measures in place to protect data gathered by CCTV cameras. A further example is ensuring there is no bias in AI-led enforcement systems.

Justice concerns the fair social distribution of resources — in this case road capacity and data. According to Floridi et al. (2018), "AI should promote justice and seek to eliminate all types of discrimination". Justice applies to all road users. This includes those accused of driving on bus lanes, who are also entitled to fairness and justice when confronted with potential infractions through automated enforcement [7]. It also includes those who do not drive on bus lanes and are entitled to a fair share of the limited road capacity.

Explicability means that all outputs should be understandable to the ordinary person. The principle of explicability complements the other four [1]. For example, if a local authority fines a citizen automatically using camera technology, it should explain what the transgression was and where it occurred. There should also be transparency and accountability regarding data usage. However, this drive to be explainable may involve recording and saving a wider sweep of footage to take driving circumstances into account, which potentially compromises the privacy and autonomy of those nearby.

As we have seen, there are conflicts and dependencies within the five principles. Moral issues arise when these principles conflict with each other [2,3]. Autonomy maximises benefits and minimises nonmaleficence within a context of justice. Beneficence is maximised when the other three principles hold true. Similarly, nonmaleficence is maximised when benefits, autonomy and justice are high. It is thus best to consider principlism, not as a set of theories that guide correct action, but rather, as procedures that help one's decisions and actions to achieve an acceptable degree of moral justification [8]. We can see that there is no simple answer, and a balance has to be struck between several opposing forces to find an ethical solution to the problem.

2.2. Benefits

There are many benefits to providing automated enforcement on bus lanes. It enables public transport to flow and people to reach their destinations on time. Bus lane enforcement improves speed and reduces variability. This increases patronage and benefits the less well-off and socially excluded, who tend to travel by bus [9–11]. Balcombe et al. (2003) state that improved public transport speed and reliability encourages modal shift from cars, which reduces emissions [12] and creates less congestion on roads. According to Snow (2017), automated enforcement promises to deliver speed and cost-effectiveness for police forces and local authorities with tight budgets. It also helps to promote sustainable modes of travel [13].

Data from cameras on bus lanes can also deliver improved safety [14,15]. Equally, the International Transport Forum (2015) claims, "Safety is one area that will benefit significantly from vehicle, infrastructure and user-based data".

2.3. Risks

While bus lane enforcement helps to mitigate risks such as those associated with the environment, social inequality and congestion, it can simultaneously create new risks. These are complex socio-technical risks that cross several socio-economic contexts and can be classified into technical, governance, public perception and legal categories [16,17].

2.3.1. Technical Risk

Technical risk is created when data are captured and have to be managed. There are many examples of this type of risk, such as cybersecurity and privacy. Cybersecurity for CCTV cameras is an area of concern. Zero-day bugs are a new paradigm [18] exposed up to 800,000 CCTV cameras to hackers who could plant malware or manipulate video feeds [19]. Hackers could gain access via a camera to a network with business data, steal user names and passwords to other systems, potentially gaining super-user status and carrying out attacks on other networked systems [20]. In addition, large numbers of cameras can be used for a denial of service attack [21]. Research by Cusack and Tian (2017) also concludes that IP cameras are vulnerable to exploitation [22].

2.3.2. Governance Risk

According to Cunneen et al. [16,17,23,24], the deployment of an emerging technology creates many complex challenges for governance regimes. Governance risk is exacerbated by a lack of clarity about what the best forms of governance are for AI applications, such as automated bus lane enforcement. Nemitz (2018) contends we need "a new culture of technology and business development for the age of AI which we call rule of law, democracy and human rights by design"[25]. He states that not regulating AI by law would "effectively amount to the end of democracy"[25]. However, top-down governance tends not to keep pace with AI development [26–28]. Human-in-the-loop is used for some implementations, e.g., a human operator in Scotland reviews video footage of an infringement using policy guidelines before deciding whether or not to send a fine [29]. However, self-governance and self-regulation are insufficient, as shown by scandals such as CRISPR and Cambridge Analytica [30]. User consent is typically not informed consent [31]. Indeed, O'Neill (2002) describes how consent has become a tool to mitigate commercial risk rather than to foster transparency [32]. Data commodification has flourished because these three methods have failed. In bottom-up governance, if AI engineers and designers are trained to make informed ethical decisions, this helps to mitigate risk.

The different types of governance approaches make bus lane enforcement a non-trivial area in which to manage risk. In addition, transport governance is typically fragmented and shared among different bodies such as local authorities, private sector, government and law enforcement. This increases the complexity of creating an integrated ethical framework.

2.3.3. Public Perception Risk

Cunneen at al. (2019) highlight the serious risks associated with negative public perception of new technologies [16]. To manage these risks, local authorities should ensure that citizens buy into the use of camera-based enforcement. Snow (2017) comments that punishments used for road safety violations detected on camera are similar to those used for less dangerous offences, such as unauthorised bus lane use [7]. He believes this offends our sense of proportionality and justice. Citizens in the UK and New Zealand have voiced concerns over a perceived rigid application of automated bus lane enforcement penalties. In the UK, fines have been levied when cars have strayed into the bus lane, which may occur, for example, when making way for an ambulance. Lack of transparency was in evidence when the Hackney Council declined to disclose their policy to the public on foot of a freedom of information request and had to be instructed by the UK Information Commissioner to disclose their code of practice [33]. There are also concerns cited by Mc Kibben (2014) that bus lane enforcement is perceived as a cash cow for councils in the UK while Price (2019) in New Zealand describes concerns that rules for motorists are unclear, which drives up the number of infringements and fines collected [29,34]. Cater (2012) cites Anderson, a spokesman for the American Automobile Association, who accuses the

Washington city government of using cameras to balance its budget "on the backs of motorists" [35].

Snow (2017) maintains that public policy in the UK is caught between embracing technology and the people's perception that widespread automated enforcement is untrustworthy and conducted to raise revenue [7]. To counter these claims, authorities need to ask a series of questions: is enforcement necessary, does this enforcement need to be automated, and how can the process of punishment be fair and appropriate or how can enforcement be viewed positively?

2.3.4. Legal Risk

In many jurisdictions, including Ireland, a legal change is required in order to enable automated bus lane enforcement. Automated bus lane enforcement was introduced in London in the mid 1990s and spread, following new regulations, to broader England and Wales in 2000. In Scotland, enabling legislation was enacted in 2012 [29].

However, successfully passing the relevant legislation is not all plain sailing. As described by Groover (2019), a bill to allow automated enforcement in Seattle failed due to privacy concerns as well as concerns over tourists being confused by street laws and subsequently fined [36]. The municipality of Bologna also encountered legal challenges when implementing a mobile automated enforcement system and had to cease implementation. Their legal framework only permitted the use of fixed cameras rather than the mobile system they were planning to use [37–39].

Authorities must ensure that GDPR provisions are followed to avoid issues after rollout. For example, the UK's Information Commissioners Office judged the use of five traffic-monitoring cameras in the town of Royston as unlawful and excessive, as they resulted in everyone entering the town being recorded, with no privacy impact assessment carried out. The judgement continued that the use of ANPR must be proportionate to the problem being addressed [40]. These are examples of where a technology solution requires and supports the fast-tracking of legal supports.

2.4. Data Privacy Issues

Privacy issues can arise when personal data are generated during camera-based enforcement. Effective data privacy depends on correct methods of data handling, consent, notice and regulatory obligations [41]. This includes when or how data are shared or collected as well as complying with regulations such as GDPR. These issues are explored further below.

2.4.1. Data Sharing

Vallance (2019) states that "there are clear benefits and savings to be made from data being shared safely between transport planners, operators and users"[42]. While AI benefits for traffic management are significant [43], human-led data policies and standards are fundamental to avoid breaches of trust, privacy and security for citizens and maintain a credible global presence [16]. The Asilomar Principles (2017) further state, "People should have the right to access, manage and control the data they generate, given AI systems' power to analyse and utilise that data"[44]. Data ownership raises many ethical issues linked to data monetisation, informed user consent and potential identity theft. Clear data ownership rules should exist to define who owns the data and who is permitted to access it, in which situations.

The International Transport Forum (2017) states, the "fusion of purposely-sensed, opportunistically-sensed and crowd-sourced data generates new knowledge about transport activity and flows. It also creates unique privacy risks"[45]. State support is typically necessary to access city infrastructure data. This is in place for many cities worldwide who

are piloting such projects. As cities grow, such technology will become inevitable, and regulation is needed to prevent abuse by state or corporate actors.

2.4.2. Data Collection

Data collection involves gathering quantitative and qualitative information to evaluate outcomes or create actionable insights. It requires a straightforward process to make sure the data collected are clean, consistent, and reliable. Creating a process involves deciding goals, identifying data requirements, deciding how to collect data, and finally defining a way to execute the most important aspects of your data collection program [46].

2.4.3. GDPR

Article 5 of GDPR identifies seven key principles of data protection. (Data Protection Commission, 2018) which are outlined below.

Lawfulness, Fairness and Transparency

Personal data should be processed in a legal and fair way. It should be transparent to people that their personal data are being gathered and to what degree it will be processed. Information and communication relevant to personal data processing should be accessed easily and be understandable.

Purpose Limitation

Personal data should only be gathered for "specified, explicit, and legitimate purposes" decided when the data are collected and not processed afterwards in a way that does not match those purposes. Camera location therefore needs careful consideration to justify an individual's reasonable expectations of privacy. Archiving of these data in the public interest is, however, permitted.

Data Minimisation

Personal data processing must be adequate, relevant as well as constrained to what is required and which could not reasonably be obtained in other ways. This requires limiting the storage period to a strict minimum.

Accuracy

Data controllers must ensure the accuracy of personal data and that any incorrect personal data are corrected in a timely manner, within reason. In particular, controllers should accurately record information and its source.

Storage Limitation

The storing of personal data should be carried out in a way which identifies subjects for as long as required, for the relevant reasons. Limits to storage durations should be set up by the controller for deletion or regular audit.

Integrity and Confidentiality

Personal data should be processed in a secure and confidential way. This includes mitigating against access, which is neither authorised nor lawful, and against loss by accident, destruction or damage, using suitable technical or organisational methods.

Accountability

Finally, the data controller must be able to show evidence to the Data Protection Commissioner that they comply with all of the above Principles of Data Protection.

2.5. Privacy and Contextual Integrity

Data commercialisation is big business and there is now a pressing need to understand the changing phenomenon of data commercialisation and privacy [16,47]. The traditional framework used to define the approach to privacy protection is threefold. It involves limiting citizen surveillance by government agents, limiting access to personal information and disallowing violations of personal or private places. However, according to Nissenbaum (2004), this is unsuitable for the case of public surveillance as it is too general [48]. Instead, she coined the term "contextual integrity" and uses it as a measure for data privacy. She posits that contextual integrity is the privacy benchmark of the information age. Contextual integrity links sufficient privacy protection to norms of contexts as well as the appropriate information gathering and flow within that context. It has at its heart a tenet that life is governed by "norms of information flow" [48–51]. This means that data gathering, and sharing should be suitable for that context and should be in line with how information is typically distributed in that context. Bennett (2011) agrees that people have a right to have their expectations met about how their personal information flows [52]. These flows take into account and support social life principles, which include the moral and political.

Nissenbaum (2004) describes two "informational norms that govern these contexts of social life, namely, appropriateness and distribution"[48]. Appropriateness decides what information is suitable to reveal in a particular context e.g., facial profiling of pedestrians would not be relevant information for a local authority enforcing bus lanes; however, capturing licence plate information of a bus lane transgressor is appropriate. Distribution refers to information transfer from one party to another. For instance, a local authority may share an image of a transgression with the car owner but may not share an image of another unconnected transgression. A breach of privacy occurs when either norm is violated. Nissenbaum (2004) argues that public surveillance "violates contextual integrity; as such, it constitutes injustice and even tyranny"[48].

Given that contextual integrity is suited to assessing privacy in a surveillance situation such as camera enforcement, it will be used to assess use cases for privacy issues in later sections.

2.6. Camera Enforcement Use Cases

It is instructive to examine examples of cameras enforcement where the environment is shared in order to impose fines. Cities use a variety of risk mitigation strategies such as facial obfuscation, access controls or privacy layers. Studying these solutions can help to point us towards potential best practices for automated enforcement of Dublin bus lanes.

2.7. Ethical Risk Mitigation — Recommended Solutions

As Cunneen et al. (2019) caution, one-size-fits-all AI conception is ill-advised, as the risks and issues vary across use cases. Instead, industries need specific regulations for their domains [16].

To mitigate concerns about privacy, the use of encryption techniques in general [53] and specifically in relation to RGB images [54,55] is improving such as open algorithms, which enable data to be analysed without being shared. Innovations in key based authentication, which enables data providers to define how data are used and by whom is growing in applications [56,57]. Cusack and Tian (2017) suggest a range of measures, such as changing default passwords, encryption, updating anti-virus software, regular auditing and changing management controls [22]. Such solutions help reduce the risk of undercapitalising on AI benefits while protecting societal values.

The EU-funded LeMO Project (2019) recommends the following actions to enable the use of big data in the transportation industry [58].

1. Regulation interventions by means of legislation, adopting standards or soft law. This includes recognising contradictions between regulation requiring hard and fast choices, and ethics which varies between and within societies and over time;
2. Ethics-by-design, ensuring that systems or applications are designed to make ethical decisions. This includes taking into account the perspective of both software developers and users;
3. Ethics-by-design enhanced by self-regulation. This combined approach is more flexible and adaptable to technology changes. It includes creating ethical codes of conduct and recommends EU oversight in creating the ethical framework. Suggested implementation principles include addressing asymmetries in information col-lection, limits on the repurposing of data, ability to opt-out of tracking and accountability. Privacy-enhancing technologies (PET's) can also be used, such as anonymisation, pseudonymisation and de-identification of data, although the risk of re-identification must be mitigated.

Society must decide how to deploy AI technologies in ways that respect human values such as equality, transparency, privacy and freedom, and all actors along the causal chain should be involved. Humanity needs open and informed debate about how to evolve AI so that all of society benefits. This will require more transparency and explainability regarding both the algorithms and the commercialise activities that relate to AI innovations [59].

3. Ethical Framework Development

The purpose of rolling out an ethical solution to automated bus lane enforcement is primarily to support the government's economic goals by having an efficient bus transport system, while reducing the risk of privacy violations from enforcement. This promotes a fairer, more ethical society, which seeks to capture the right to privacy of any people recorded who are not part of the infringement.

The problem of ethical bus lane enforcement cannot be solved by creating general rules, rather it needs a thorough analysis guided by a framework to analyse complex information flows. This analysis will contextualise the ethical dilemma and apply the above literature review and use cases to the Dublin bus lane case. It will identify options and evaluate each in terms of how they solve risks. The best option is then selected. The output of this framework and analysis is a template of the minimum data required to implement ethical automated bus lane enforcement using a privacy-by-design approach.

3.1. Identify the Ethical Dilemma

As we have shown, bus lanes need to be enforced to operate effectively. Unauthorised bus lane use undermines the effectiveness of the bus lane tool. Enforcement can be manual or automated. Manual methods are ineffective as they don't scale and require scarce, expensive resource. Therefore, the aim is to provide an automated solution that mitigates the risk of unauthorised use. This in turn creates new ethical risks, such as privacy, technical and legal, etc. The question is, how to mitigate these risks which have undermined bus lanes elsewhere.

3.2. Use Data to Make an Informed Decision

Bus lane enforcement in Dublin brings many benefits, as it enables public transport to travel faster and promotes a modal shift from car to bus, which reduces greenhouse emissions. The bus is a more sustainable mode of transport compared to private cars and good public transport infrastructure will help to promote economic growth. Dublin has no underground, with a limited train and light rail network, making the efficient running

of the bus network even more crucial. Bus travel is also inclusive, particularly for the poorest in society.

However, new risks are created which need to be mitigated. This risk mitigation (Table 1) assessment is compiled from theory, use cases in the Appendix A (Table A1) and proposed solutions to issues, as identified in the literature review.

Table 1. Risk Mitigation Measures for Dublin.

Technical Risk	Use the minimum amount of data possible to achieve the enforcement benefits and store it for the minimum time necessary.
	Ensure data is secure both when stored and in transit.
	Ensure the maximum amount of data is processed at the edge and the minimum of data is sent for central processing.
	Implement security measures, e.g., changing access passwords, encryption, updating anti-virus software, regular auditing and change mgmt. controls for devices storing CCTV footage.
	Review and test access controls regularly. Enhance or upgrade security measures as necessary.
PR Risk	Promote the benefits of automated camera enforcement.
	Have a transparent appeal process with a culture of fairness and appropriateness.
	Audit bus lane usage and share statistics and stories about unauthorised usage with consequent impacts to the travelling public.
	Hold public consultations in advance of rollout and communicate results as well as actions taken.
	Provide clear, consistent guidelines about what constitutes a breach.
	Provide transparency about the reason for a fine, while protecting the privacy of others unrelated to the incident.
	Have a human-in-the-loop for appeals.
	To deter repeat offenders, use increased fines for late payment, with reduced fines for prompt payment.
	Be transparent about the use of fines, e.g., use them to fund climate change projects.
	As described by Matheson (2020), using satellite imagery to tag road features, such as bus lanes in digital maps, helps flag to drivers where bus lanes are. This helps drivers navigate in unfamiliar locations.
	Use positive reinforcement — e.g., reward law-abiding drivers randomly to encourage positive behaviour.
Governance	Ethics, privacy and human rights-by-design enhanced by self-regulation. This includes creating ethical codes of conduct.
	Train bus enforcement designers and operational personnel in ethics, privacy and risk mitigation.
	Put processes in place for organisations to monitor and support designers to develop ethical AI systems.
	Foster an integrated governance approach between relevant authorities implementing bus lane enforcement.
Legal	Ensure the legal framework in place supports the type of camera enforcement being rolled out.
	Conduct a data protection impact assessment to include stakeholder engagement and feedback. This should take into account all innocent parties in the scene who may be recorded.
	Ensure the use of cameras is justifiable in the circumstances, that alternate measures are insufficient and that the impact on individuals is proportionate.

Privacy	Record only for the time of day when the bus lane is in use (e.g. morning and evening rush hour) Sense traffic movement and record only when traffic is passing or when the lane is blocked. For cameras on buses, the driver records only in cases of unauthorised lane access by another vehicle.
	Limit automated bus lane enforcement to the busiest routes where there is a proven issue with enforcement. Stop surveillance once new behaviour is observed.
	Only retain footage where there is a violation.
	Do not sell personal data to third parties.
	Sensors and AI detect bus lane use. This is processed at the edge and discarded.
	Use obfuscation on faces and other licence plates in the scene.
	No facial recognition software to be used.

3.3. Identify Possible Options

Option 1: Current Norms (Figure 1):

1. Police guard bus lanes for a period of time without notice. Based on visual inspection, they stop any unauthorised vehicles and take licence plate and driver details. If there are mitigating circumstances, they are dealt with at the scene. Otherwise, details are transferred to a central IT system so that fines can be issued. The actors in this case are the guard and the transgressor who are visible to each other at the point of transgression.
2. Pedestrian and cyclist details in the scene are typically not taken.
3. Details of cars in other lanes in the scene are also not typically relevant and are therefore not noted.

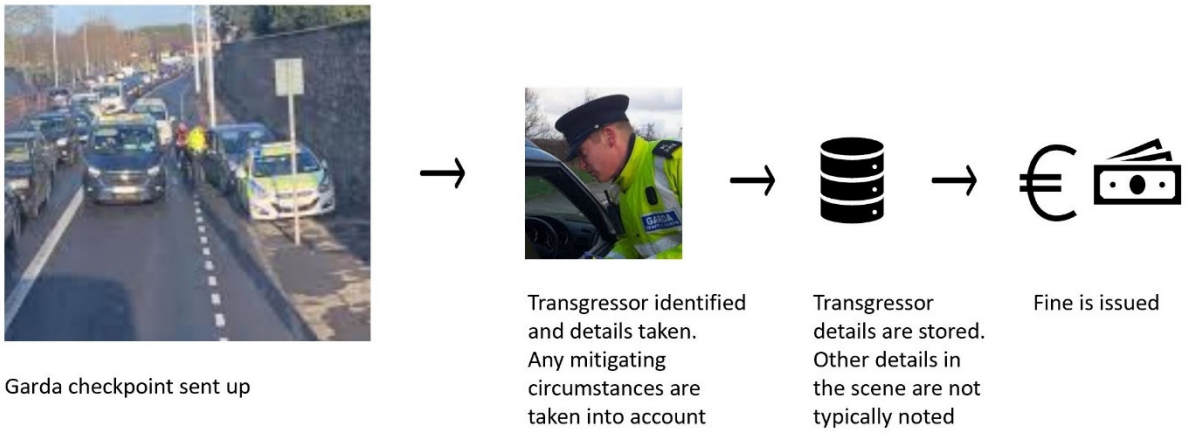

Figure 1. Current norms of bus lane enforcement.

Option 2. Bus Driver Records Scene (Figure 2):

1. There is a camera mounted on the front of the bus
2. Bus driver records infringements in the bus lane as they happen
3. Scene data are sent centrally and a fine is issued

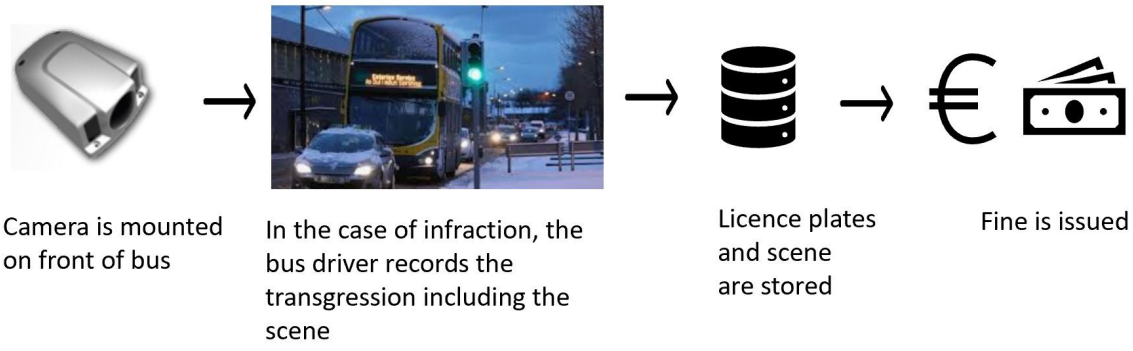

Figure 2. Bus driver records scene.

Option 3. Record ANPR (Figure 3):

1. Camera operates to record in the bus lane.
2. Camera records only licence plates of vehicles in the bus lane. It does this continuously when vehicles are present. Fine are issued regardless of mitigating circumstances, which cannot be proven in any case. All licence plate details are transferred to a central system, which compares licence plates against vehicle types to detect infringements.

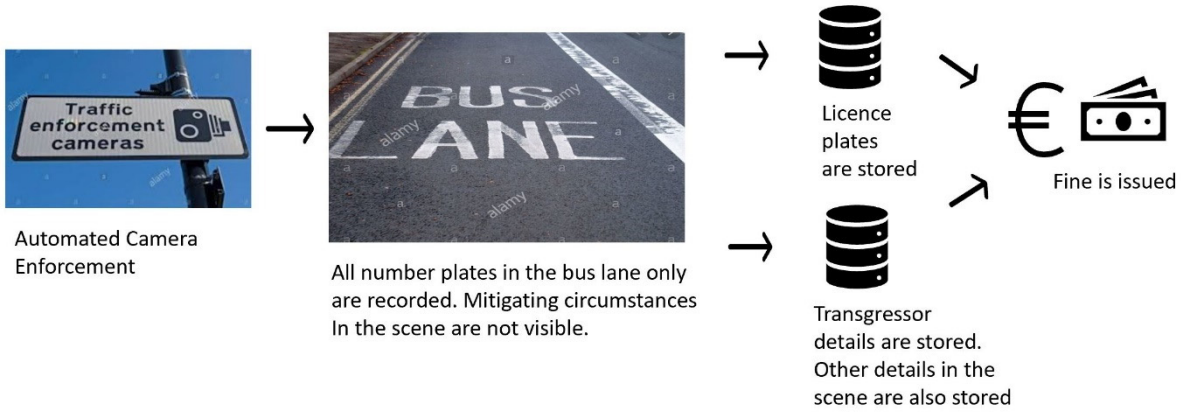

Figure 3. Record ANPR.

Option 4. Record Scene (Figure 4):

1. Camera operates to record continuously in the bus lane and wider scene to provide context into mitigating circumstances. This also captures details of other vehicles and people.
2. The footage is sent to a central system, which consults a central licence plates database to identify infringers.
3. Fines are issued with video/image clips of scene. There is a process to deal with mitigating circumstances, based on the recorded content.

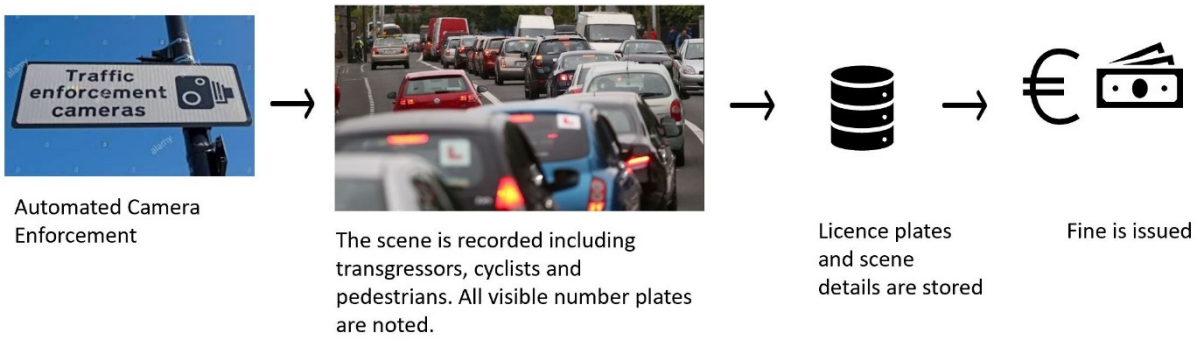

Figure 4. Record scene.

Option 5. Minimise personal data collected for an ethical solution (Figure 5):

1. Prioritise areas and times of high bus lane transgressions for enforcement. This avoids a blanket camera deployment and recording approach as well as minimising costs of the operation.
2. Detect vehicle types in the bus lane in real-time at the edge to ascertain authorised vs. unauthorised use. Discard footage if no transgressions.
3. If a transgression occurs, capture the licence plate of the transgressor.
4. Record the scene of the transgression to show circumstances. This can be a video or screenshots.
5. The licence plates of any other vehicles in the scene are not needed and should be obfuscated.
6. The facial features of anyone in the scene are not needed and should also be obfuscated.
7. The video or screenshots of the transgression are sent to a central repository for further action.

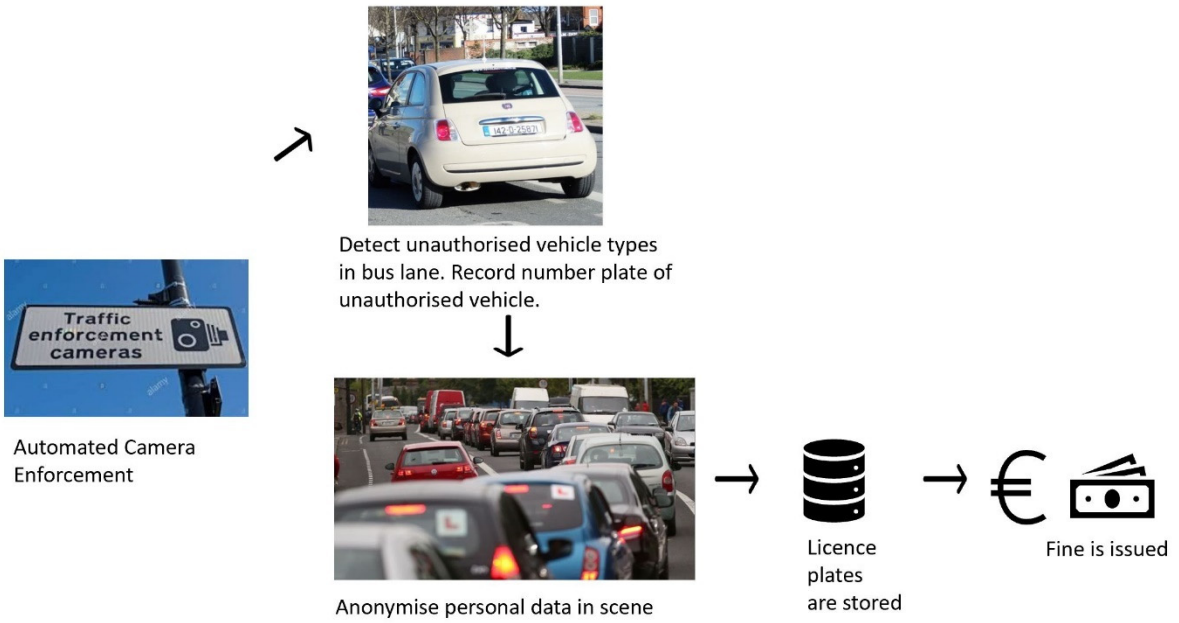

Figure 5. Minimise recording of personal data for an ethical solution.

3.4. Apply the Ethical Principles to the Options and Evaluate

Option 1, "Current norms ": We can see that information extraction and retention is relevant to the misdemeanour only. The outcome of the process is to act as a deterrent to future transgressions, thus helping to combat the problem of congestion and addressing the values, goals and purposes of enforcement. Technical risk is low for this solution, as only data relevant to the misdemeanour is captured. However, this solution requires scarce personnel and is impractical to operate at scale, which enables offences to proliferate. Thus, there is a need for alternative solutions.

Option 2, "Bus Driver Records Scene": This solution meets current norms in many ways. The bus driver only records when their bus is blocked. They may also be able to take mitigating circumstances into account as they can see the scene unfolding. They record the scene, which meets the ethical principles of fairness and explicability by demonstrating the environment and potential mitigating circumstances in which the transgression took place. However, there are two issues. Firstly, bus lane enforcement in Dublin is currently the remit of An Garda Siochana. Legislation would be required to change this. Bus drivers and their unions would then have to accept the new responsibility. This raises considerable governance and legal risk. Secondly, recording the scene without obfuscation creates a privacy risk as it changes distribution norms.

Option 3, "Record ANPR": This solution violates current norms and contravenes ethical principles of fairness and explicability by not demonstrating the environment and potential mitigating circumstances in which the transgression took place. This makes public acceptance of the solution more challenging. Without recording the scene, it can be more difficult to account for technical errors in the process, e.g., any false positives in the automated enforcement system.

Option 4, "Record scene": Current norms are being violated where pedestrians in the scene and vehicles in other lanes are recorded without giving consent or potentially being aware of it. Furthermore, all the footage is sent to a central location to detect infringements, resulting in large-scale surveillance of public space and increasing security risk. This departure from entrenched norms merits a values-based assessment. It compromises the privacy and self-determination of innocent parties while not contributing to the values, goals and purposes of the activity. Unfairly capturing the data of other road users, who could include children, raises governance, privacy and technical risk. It also breaches the ethical principle of justice and infringes on the ethical principle of nonmaleficence by causing unjustifiable harm and reducing the autonomy of other people in the scene. The innocent parties have no choice regarding the capturing of their licence plate number or facial details. This method may also be deemed to be capturing an excessive amount of data and thus fall foul of GDPR's requirement of proportionality.

In addition, we can see that although people are out in public, the norms of information flow in this context have changed. This personalised data can be captured, identified via facial profiling, tracked across locations in the case of networked or mobile cameras, transported, aggregated with other personalised data, further processed and shared. Therefore, people can be justifiably concerned about the lack of privacy, even when just captured out in public.

The purpose of bus lane enforcement is to keep bus lanes free, which increases their speed, predictability of arrival and encourages increased ridership. Harnessing data about transgressors is a necessary part of this endeavour. Harnessing data about others in the scene does not contribute to this aim.

Option 5: "Minimise personal data collected for an ethical solution." This option stays as close to existing norms as possible while allowing for automation. The design aims to bridge the ideal technical solution, which has unimpeded access to data needed for enforcement and the ideal ethical solution, which addresses the ethical challenges in order to optimise benefits. It takes into account issues and risks, as described in the examples above, and is a less invasive and more ethical method of achieving the same goals. This method avoids blanket capturing of licence plates in the scene. It ensures the minimum

amount of personal data is captured and sent to a central repository for further action. Further, it ensures that only relevant data is captured and data is stored for the minimum amount of time. The only identifying data sent or stored is the licence plate of the transgressor.

3.5. Make Decision

As Nissenbaum (2011) indicates, new information flows can be seen as preferable to old flows if they are more effective at achieving values, ends and purposes that might be paramount in a transportation context, such as predictable journey times, green transportation and fair resource use etc [49]. If it is decided instead that traditional information flows are more preferable, then contextual integrity could be said to have been breached. Key to this understanding is a belief "that a right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information", Nissenbaum [49].

Option 5 focuses on providing an ethical solution that provides more preferable information flows to the norm, as it uses technology to provide a more effective way of achieving benefits while staying true to ethical values. The solution complies with the ethical principle of beneficence as it promotes sustainable travel for the well-being of humanity, while mitigating many risks associated with automated camera enforcement. Thus, it is the chosen solution for proof of concept implementation.

3.6. Evaluate Decision for New Risks

While the chosen solution is the optimal balance between the ideal technical and the ideal ethical solution, it creates new risks. It is technically more complex to implement, which adds cost. However, this is unlikely to cost as much as new road infrastructure would. Other risks include AI detection errors caused by varying light and weather conditions. Augmenting the solution with infrared detection and training on larger, more varied datasets can help to mitigate this. A human-in-the-loop, as used in Scotland, can also help to assess if a fine is valid or not. This also reduces public relations risk. Although the scene is recorded, anonymisation reduces privacy risk. However, it is necessary to select anonymisation techniques that cannot be easily reversed.

The focus is on providing an ethical solution that provides more preferable information flows to the norm, as it uses technology to provide a more effective way of achieving benefits while staying true to ethical values. The solution complies with the ethical principle of beneficence, as it promotes sustainable travel for the well-being of humanity, while mitigating many risks associated with automated camera enforcement. Thus, it is the chosen solution for implementation.

4. Conclusions and Future Research

This paper is intended to stimulate debate about the effectiveness and ethics of using AI technologies like camera-led bus lane enforcement as an alternative to road widening. The solution proposed is not intended to be definitive; rather, it is a proof of concept, which contributes to that debate. There is a planned two billion spend in Ireland in order to build new bus lanes by widening roads. However, existing bus lanes are not effective, as they are manually enforced; there is no plan to automatically enforce the new bus lanes and thus no proof that the spend will be effective. It would make sense before undertaking the cost of widening roads to first make existing bus lanes more effective. The best way to do this is to use AI technology to improve enforcement and to investigate other methods of using technology to decrease congestion. Given the prevalence of traffic congestion and the global footprint of bus lanes, this is an important topic with real societal impact. While there is room for further development, this research makes two significant contributions:

Risk analysis: detailed research to identify and reduce the risks associated with automated bus lane enforcement implementations.

Privacy-by-design: a novel way to protect the personal information of road users while being fair and transparent to potential transgressors. This includes a template of the minimum data required to implement ethical automated bus lane enforcement using a privacy-by-design approach.

This research invites further investigation in several areas. It would be interesting to install cameras on Dublin's buses and compute bus delays due to infringement. This could be a useful tool for increasing public perception of enforcement. The concept could be extended to detecting cycle lane infringements. The main driver for doing this would be cyclist safety. A risk analysis of automated cycle lane enforcement could be carried out and a privacy-by-design enforcement solution proposed. In addition, autonomous vehicles, which are also equipped with cameras, share some ethical risks with automated bus lane enforcement. It would be interesting to explore these risks in the context of autonomous vehicles and develop a privacy-by-design approach to handling them using the same ethical framework proposed here.

Author Contributions: Conceptualization, C.L., J.N. and M.C.; Data curation, C.L.; Formal analysis, C.L.; Investigation, C.L.; Methodology, M.C.; Supervision, J.N. and M.C.; Writing – original draft, C.L.; Writing – review & editing, J.N. and M.C. All authors have read and agreed to the published version of the manuscript.

Funding: No funding applicable

Institutional Review Board Statement: Not applicable

Informed Consent Statement: All contributors have given their informed consent to the research and publication.

Data Availability Statement: Data is available on request.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Global use cases of camera enforcement.

Enforcement	Risks	Risk Mitigation Strategies in Practice
Traffic Enforcement Utrecht	Governance Legal PR Privacy Technical	General: Fines of up to EUR 431 can be levied. Nehra (2019). Process in place for recourse. Increased fines for late payment. Digital cameras mean fine arrives within 7 days. (CJIIB, 2019). Data collected: ANPR is used. No facial data is captured. Bus lane enforcement is limited to busiest routes, which limits surveillance. (CJIIB, 2019). Data storage: Vehicle registration details from vehicles passing an ANPR camera may be retained for up to four weeks. (Government of the Netherlands, 2018). Access controls: In addition to Dutch police, the Dutch intelligence services have access to this database. (PrivacyFirst, 2019)
Bus Lane Enforcement Singapore	Legal Privacy Technical	Data collected: Licence plate information is used for identification. Camera on bus operated by driver who captures blocking incident as it happens, reducing wide-spread surveillance. (Barter, 2008). Access controls: Strict rules are in place regarding access and sharing of video data.
Bus Lane Enforcement UK	Governance Legal PR Technical	General: Prompt payment cuts fine in half. Poor public perception of bus lane fines as 'money earners.' Perception of inconsistent guidelines regarding left turns. The vehicle owner, not the driver, is typically responsible for payment. Human-in-the-loop checking results in reduces PR risk. Data sharing: If a user appeals a penalty, their data will be shared with the relevant enforcement authority. This includes the adjudicator (a data

		controller) who determines the outcome. It may include the driver and vehicle licensing agency (DVLA) to clarify the lawful owner of the infringing vehicle. It also includes Northgate Public Service Ltd, a third party provider, which hosts the appeals management and back-office systems. (London Tribunals, 2019) Data storage: Hard copy documents, which are digitisable, are destroyed 3 months after receipt. Hard copy documents, which are not digitisable, are destroyed 6 months after the last action on a case. Electronic copies of documents are deleted 1 year after the last action on a case. Case files are deleted 7 years after the last action.
Millbank, London, UK	Legal Privacy Technical	Data collected: Sensors use AI to gather video which detects road users and their transport method. The technology can detect cyclists, pedestrians and traffic such as cars, vans and buses. The data is processed at the edge and then discarded. Data storage: None. Data sharing: In the future, the system will be integrated to London's traffic management systems. This will provide real-time data.
M50 Toll road Ireland	Legal Privacy Technical	Data collected: Emovis Operations Ireland operate toll services on behalf of Transport Infrastructure Ireland and may gather data directly from end-users such as: "Full Name, Address Details, Email Address and Phone Number". They are permitted to gather additional data such as: "licence plate number, journey reference number, eFlow account number, bank statement, log book and payment details, credit/debit card or direct debit". Personal data can also be gathered indirectly, such as "IP address or licence plate number". They receive, for example, data from the National Vehicle File (NVDF) through the Driver Vehicle and Computer Service Division (DVSCD) [60].
The Dublin Airport Authority Ireland	Legal Privacy Technical	General: The Dublin Airport Authority (DAA) [61] operate CCTV cameras in Dublin Airport's buildings and surrounding areas. Data collected: Personal data may be recorded by CCTV cameras. CCTV data may also track or analyse passenger or vehicle flows. Data shared: It may be a requirement for the DAA to share visitor data to meet legal and regulatory obligations, analyse safety or security issues or crime. They may share personal CCTV data with: • An Garda Síochana or the Irish Aviation Authority • Third parties operating shops, or providing passenger services, such as airlines or handling agents where a legal obligation exists. All personal data gathered for the stated reasons are processed within the European Union (EU) or the European Economic Area (EEA) and will never be moved to other countries outside of these. Data storage: They keep CCTV recordings for thirty days. If CCTV recordings are determined to be linked to a formal occurrence, it is stored for six years from the date the incident is reported or longer, until the incident has been fully investigated. Access controls: The DAA apply access controls at different levels to restrict viewing of personal data to employees and third parties requiring it. They examine "security, data protection policies and procedures" frequently, ensuring sufficient operational security [61].

References

1. Floridi, L.; Cowls, J.; Beltrametti, M.; Chatila, R.; Chazerand, P.; Dignum, V.; Luetge, G.; Madelin, R.; Pagallo, U.; Rossi, F.; et al. AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds Mach (Dordr)* **2018**, *28*, 689–707.
2. Beauchamp, L.T.; Childress, J.F. Response to Commentaries. *J. Med. Philos. A Forum Bioeth. Philos. Med.* **2020**, *45*, 560–579.
3. Beauchamp, L.T.; Childress, J.F. *Principles of Biomedical Ethics*; Oxford University Press: New York, NY 10016, USA, 2001.
4. Beal, A. In China, Alibaba's data-hungry AI is controlling (and watching) cities., in WIRED. 2018. Available from: https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur (accessed on15 August 2019).
5. Canellopoulou-Bottis, M.; Bouchagiar, G. Personal data v. Big data: Challenges of commodification of personal data. *Open J. Philos* **2018**, *8*, 206–215.
6. Gates, K.A. *Our Biometric Future*; New York University Press: New York, NY 10003-4812, USA, 2011.
7. Snow, A. *Automated Road Traffic Enforcement: Regulation, Governance and Use*; Royal Automobile Club Foundation: London, UK, 2017.
8. Hine, K. What is the outcome of applying principlism? *Theor. Med. Bioeth.* **2011**, *32*, 375–388.
9. Winston, C. Government failure in urban transportation. *Fisc. Stud.* **2000**, *21*, 403–425.
10. Kim, K.S.; Dickey, J. Role of urban governance in the process of bus system reform in Seoul. *Habitat Int.* **2006**, *30*, 1035–1046.
11. Houston, D.J. Buses, Trains, and Automobiles: Facing the Challenges of Urban Transportation. *Public Perform. Manag. Rev.* **2001**, *25*, 251–255.
12. Nanaki, E.; Koroneos, C.; Roset, J.; Susca, T.; Christensen, T.; Hurtado, S.D.G.; Rybka, A.; Kopitovic, J.; Heidrich, O.; López-Jiménez, P.A. Environmental assessment of 9 European public bus transportation systems. *Sustain. Cities Soc.* **2017**, *28*, 42–52.
13. Balcombe, R.; York, I.; Webster, D. *Factors Influencing Trip Mode Choice*; Transport Research Laboratory: Wokingham, UK, 2003.
14. Bu, F.; Chan, C.-Y. Pedestrian detection in transit bus application: Sensing technologies and safety solutions. In Proceedings of the IEEE Proceedings. Intelligent Vehicles Symposium, Las Vegas, NV, United States, 6–8 June 2005.
15. Bhandari, R.; Raman, B.; Padmanabhan, V.N. Fullstop: A camera-assisted system for characterizing unsafe bus stopping. *IEEE Trans. Mob. Comput.* **2019**, *19*, 2116–2128.
16. Cunneen, M.; Mullins, M.; Murphy, F. Artificial Intelligence Assistants and Risk Framing a Connectivity Risk Narrative draft. AI & Society. **2020**. 35. 10.1007/s00146-019-00916-9.
17. Cunneen, M.; Mullins, M.; Murphy, F. Autonomous Vehicles and Embedded Artificial Intelligence: The Challenges of Framing Machine Driving Decisions. *Appl. Artif. Intell.* **2019**, *33*, 706–731.
18. Kuehn, A.; Mueller, M. Shifts in the cybersecurity paradigm: Zero-day exploits, discourse, and emerging institutions. In Proceedings of the 2014 New Security Paradigms Workshop, Victoria, BC, Canada, September 15–18, 2014.
19. Mansfield-Devine, S. Weaponising the internet of things. *Netw. Secur.* **2017**, *2017*, 13–19.
20. Costin, A. Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, 2016.
21. Hilt, S.; et al., Worm War: The Botnet Battle for IoT Territory. documents. trendmicro. com (), 2020: P. 30. Available from: https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf (accessed on 15 August 2021)
22. Cusack, B.; Tian, Z. *Evaluating IP Surveillance Camera Vulnerabilities*; 2017. The Proceedings of 15th Australian Information Security Management Conference, 5–6 December, 2017, Edith Cowan University, Perth, Western Australia. 25–32.
23. Cunneen, M.; Mullins, M.; Murphy, F.; Gaines, S. Artificial Driving Intelligence and Moral Agency: Examining the Decision Ontology of Unavoidable Road Traffic Accidents through the Prism of the Trolley Dilemma. *Appl. Artif. Intell.* **2019**, *33*, 267–293.
24. Cunneen, M.; Mullins, M.; Murphy, F.; Shannon, D.; Furxhi, I.; Ryan, C. Autonomous Vehicles and Avoiding the Trolley (Dilemma): Vehicle Perception, Classification, and the Challenges of Framing Decision Ethics. *Cybern. Syst.* **2020**, *51*, 59–80.
25. Nemitz, P. Constitutional democracy and technology in the age of artificial intelligence. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2018**, *376*, 20180089.
26. Hagemann, R.; Skees, J.H.; Thierer, A. Soft law for hard problems: The governance of emerging technologies in an uncertain future. *Colo. Tech. LJ* **2018**, *17*, 37.
27. Sadaf, R.; et al., Algorithmic Trading, High-frequency Trading: Implications for MiFID II and Market Abuse Regulation (MAR) in the EU. High-frequency Trading: Implications for MiFID II and Market Abuse Regulation (MAR) in the EU, 2021. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3846814 (accessed on 15 August 2021)
28. Marchant, G.E. Addressing the pacing problem. In *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 199–205.
29. McKibbin, D. *Enforcing Bus Lanes. Research and Information Service Briefing Paper*; 2014. Available from: http://www.niassembly.gov.uk/globalassets/documents/raise/publications/2015/regdev/2015.pdf (accessed on15 August 2019)
30. Frahm, N.; Doezema, T. Are Scientists' Reactions to 'CRISPR Babies' About Ethics or Self-Governance? *STAT* **2019**, *28*. Available from: https://bioethics.com/archives/45467 (accessed on 15 August 2021)
31. Luger, E.; Moran, S.; Rodden, T. Consent for all: Revealing the hidden complexity of terms and conditions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Paris France, 27 April–2 May 2013.

32. O'neill, O. *A Question of Trust: The BBC Reith Lectures 2002*; Cambridge University Press: 2002. Available from: https://www.bbc.co.uk/programmes/p00ghvd8 (accessed on 15 August 2021)
33. Verkaik, R. Stuck in traffic? Nipping into the bus lane is likely to cost you, in Independent UK. 2006. Available from: https://www.independent.co.uk/life-style/motoring/features/bus-lanes-and-law-5335611.html (accessed on 15 August 2021)
34. Price, K. AA hits out at high number of bus lane tickets doled out to Auckland motorists, in NZHerald. 2019. Available from: https://www.nzherald.co.nz/nz/auckland-transport-bus-lane-trial-nets-22m-in-fines-on-newmarket-street-in-three-months/WV7M2D34A6LGNS4REDYQFSIDPY/ (accessed on 15 August 2021)
35. Cater, F. *Motorists to Urban Planners. Stay in Your Lane*; 2012. Available from: https://www.npr.org/2012/07/18/155917197/motorists-to-urban-planners-stay-in-your-lane (accessed on 15 August 2021)
36. Groover, H. *Transportation Scorecard: What Won, Lost in This Year's Washington Legislative Season*; 2019. Available from: https://www.seattletimes.com/seattle-news/transportation/transportation-scorecard-what-won-lost-in-this-years-washington-legislative-session/ (accessed on 15 August 2021)
37. Van Rooijen, T.; Quak, H. City logistics in the European CIVITAS initiative. *Procedia-Soc. Behav. Sci.* **2014**, *125*, 312–325.
38. Dziekan, K. Evaluation of measures aimed at sustainable urban mobility in European cities–Case study CIVITAS MIMOSA. *Procedia-Soc. Behav. Sci.* **2012**, *48*, 3078–3092.
39. Brůhová-Foltýnová, H.; Jordová, R. Contribution of the CIVITAS Initiative to local policies and better policy environment. Available from: https://www.researchgate.net/publication/332383704_Contribution_of_the_CIVITAS_Initiative_to_local_policies_and_better_policy_environment (accessed on 15 August 2021)
40. Espiner, T. Police Number Plate Camera Scheme Broke the Law in Royston. BBC News, July, 2013. 24. Available from: https://www.bbc.com/news/technology-23433138 (accessed on 15 August 2021)
41. Herrmann, D.S. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*; CRC Press: 2007.
42. Vallance, P.; Norman, J. *A Time of Unprecedented Change in the Transport System*; Government Office for Science: 2019.
43. Agarwal, P.K.; Gurjar, J.; Agarwal, A.K.; Birla, R. Application of artificial intelligence for development of intelligent transport system in smart cities. *Int. J. Transp. Eng. Traffic Syst.* **2015**, *1*, 20–30.
44. Asilomar, A. Principles. (2017). in Principles developed in conjunction with the 2017 Asilomar conference [Benevolent AI 2017]. 2018. Available from: https://futureoflife.org/ai-principles/ (accessed on 15 August 2021)
45. By, S. *ITF Transport Outlook International Transport Forum*; 2017. Available from: https://www.oecd-ilibrary.org/transport/itf-transport-outlook-2017_9789282108000-en (accessed on 15 August 2021)
46. Li, T.; Vedula, S.S.; Hadar, N.; Parkin, C.; Lau, J.; Dickersin, K. Innovations in Data Collection, Management, and Archiving for Systematic Reviews. *Ann. Intern. Med.* **2015**, *162*, 287–294.
47. Cunneen, M.; Mullins, M. *Framing Risk, The New Phenomenon of Data Surveillance and Data Monetisation; from an 'Always-On'culture to 'Always-On'artificial Intelligence Assistants*; international Conference on Robot Ethics and Standards, New York, USA, 20–21 August 2018, Hybrid Worlds: 2019, p. 65.
48. Nissenbaum, H. Privacy as contextual integrity. *Wash. L. Rev*. 2004. 79, 119.
49. Nissenbaum, H. A contextual approach to privacy online. *Daedalus* 2011. 140, 32-48.
50. Nissenbaum, H. *Privacy in Context*; Stanford University Press: 2020.
51. Jannusch, T.; David-Spickermann, F.; Shannon, D.; Ressel, J.; Völler, M.; Murphy, F.; Furxhi, I.; Cunneen, M.; Mullins, M. Surveillance and privacy–Beyond the panopticon. An exploration of 720-degree observation in level 3 and 4 vehicle automation. *Technol. Soc.* **2021**, *66*, 101667.
52. Bennett, C.J. Privacy in Context: Policy and the Integrity of Social Life. *Surveill. Soc.* **2011**, *8*, 541.
53. Safi, A. Improving the security of internet of things using encryption algorithms. *Int. J. Comput. Inf. Eng.* **2017**, *11*, 558–561.
54. Ghadirli, M.H.; Nodehi, A.; Enayatifar, R. An overview of encryption algorithms in color images. *Signal Process.* **2019**, *164*, 163–185.
55. Liu, F.; Koenig, H. A survey of video encryption algorithms. *Comput. Secur.* **2010**, *29*, 3–15.
56. Sharma, K.M.; Bali, R.S.; Kaur, A. Dyanimc key based authentication scheme for Vehicular Cloud Computing. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 8–10 October 2015, Greater Noida, Delhi, India
57. Hosseinzadeh, M.; Ahmed, O.H.; Ahmed, S.H.; Trinh, C.; Bagheri, N.; Kumari, S.; Lansky, J.; Huynh, B. An Enhanced Authentication Protocol for RFID Systems. *IEEE Access* **2020**, *8*, 126977–126987.
58. Timan, T.; Mann, Z. Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In *The Elements of Big Data Value*; Springer, Cham, Switzerland, 2021; pp. 153–175.
59. Mullins, M.; Holland, C.P.; Cunneen, M. Creating ethics guidelines for artificial intelligence and big data analytics customers: The case of the consumer European insurance market. *Patterns* **2021**, *2*, 100362.
60. EFLOW. Data Protection. 2019. Available from: https://www.eflow.ie/help-guidance/faqs/the-m50-toll-road/data-protection/ (accessed on 15 August 2021)
61. Authority, D.A. Privacy Policy. 2019. Available from: https://www.dublinairport.com/privacy-policy (accessed on 15 August 2021).