Ethical Considerations in the Deployment of IoT Sensors for Autonomous Vehicle Monitoring

By Dr. André Cardoso

Associate Professor of Computer Science, Federal University of Minas Gerais (UFMG), Brazil

1. Introduction

The development and deployment of IoT devices entails complex and multidimensional issues related to privacy, security, safety, ethics, legal, and environmental considerations. The resulting heterogeneity and complexity of IoT ecosystems pose a rich and potentially confusing set of interactions among the individual systems and users, with the consequent risk of emergence of collective purposes and mechanisms for policy intervention. In order to optimally harness the individual devices in a collective take-on task, a top-down approach would have to take into account any composite functions which can be derived and to provide incentives to the device owners. Second, to avoid any unsafe and/or unethical synergistic effects — which neither a traditional bottom-up nor the mentioned top-down approach can guarantee — flexible and language-oriented soft law policies should be established to govern the collective action-states and kinematic network witnessed, adaptively and dynamically, in an 'emic' way. The authors believe that endorsing amongst the various collective interacting systems some commonly accepted soft laws is a crucial step towards managing human-centred IoT collectives in the public domain and their responsible collective behaviour [1].

The Internet of Things (IoT) promises to revolutionize the field of transportation, lead to more efficient handling of available resources and provide faster and more reliable means of traveling over any reflective variety of routes; it is expected to prevent most traffic accidents, avoiding the deaths of many people and significantly reducing the emissions from energy use and the pollution generated by transportation. Moreover, in modern smart cities, millions of devices are interconnected and generate not only data, but information, which can be used to take better decisions, reduce the costs and improve the quality of life [2]. Vehicle manufacturers and transportation authorities are embracing the ambitious goal of zero fatalities on road traffic. According to a Vision Zero approach, this can be reached by ensuring

that road traffic will have no negative effect, such as fatalities or serious injuries, on people. This holistic and multi-sectorial approach calls for continuous developments to ensure a robust framework against which the introduction of automated or connected vehicles and systems has to be assessed. When designing autonomous vehicles, different ethical questions have been posed, but such problems are not limited to technological choices, they involve societal and legal barriers and normative requirements. Therefore, a multi-disciplinary approach combines moral philosophy, legal standards, the empirical social sciences, computer science and engineering in order to achieve responsible and ethical mobility for automated and connected vehicles [3].

1.1. Background and Rationale

[4] [5]The modern essence of the Internet of Things (IoT) includes real-time monitoring and actuation subsystems including IoT sensors for autonomous vehicle monitoring and real-time monitoring of surface condition and integrity optimized by IoT devices. Outcomes from IoT sensing and actuating devices improve statistical predictive analysis and forecast for an efficient utilization of surface resources and quality control. As Environmental, Social, and Governance (ESG) and corporate social responsibility (CSR) are focal topic in the present days, the study about legislations and standards, financing and investing, running and management, and corporate culture and policy in such a holistic analysis and forecast becomes more popular. However, ethical considerations in the real-time operation and maintenance of IoT sensors are not leapt over in any detailed work.[6]Ethical considerations play a fundamental role in the development and deployment of Internet-of-Things (IoT) sensors for real-time monitoring. Using an ethical algorithmic ethic behaviour framework, the authors present a taxonomy of the issues that could arise during the conception, development, deployment, and maintenance of IoT deployments. The goal is to inform the practice for the detection and resolution of the issue as they emerge and to inform the execution of ethical software in general. The taxonomy shows a problem and analysis from practitioners. Future research should address social ethical norms, certification practices, regulatory framework, and more.

1.2. Scope and Objectives

Another crucial priority results from cars flowers of capacity, claimed features and also lineages of different features. Reasons as comfort have driven several manufacturers to

tolerate system input from car drivers but also increase evaluation offering default track the driver although he is in a position to manoeuvre the vehicle in a secured way. A final objective is to use the gathered data to identify the general feeling of the user's wear and speak the data to the IoT sliders environment [7]. "SenToolacted for an optical equipment, usable in cars, that analyses the vital parameters of car users. Sensors absorb the DNA tone, more precisely electrocardiogram and respiration traces. Images represent blood compression spoons, electromyography signs and face communication signals. Based on the described solution, user abilities are analysed by computational intelligence techniques. Intelligence benefits can be employed: to perform biometric identification, to smile the driver and to identify munus and body parts movements."

The increasing deployment of Internet of things (IoT) sensors will raise concerns about the integrity of the car's data and of the car users' privacy [ref: 27f7ccdb-8f40-4fb7-a1e0-ced6f9442f7c, ref: 2442825f-4cca-499c-90f5-85c4e52627b3]. The reason for the first ethical challenge lies in the electronic architecture of the IoT objects in cars and their deployment to process sensitive data internally which may lead to protection vulnerabilities exploited by motivated malicious actors. A regular issue about IoT ecosystem is the control and property of acquired data with the entity who obtains data, especially about sensitive data like driving. Therefore, one crucial priority is to use the collection, transmission and storage of driving behaviour data in connected or partly autonomous cars far from safety and organizational risks that might alter human free will or privacy.

2. Understanding IoT Sensors in Autonomous Vehicle Monitoring

In the scenarios imagined above, moral progress is assumed for the optimization of licensing, discrimination, insurance, and markets (pricing of new products and services), all operating in favor of AV development [8]. Various norms and codifications of the developmental scenario may emerge in feedback from experience of operation, use, calibration, and redesign suggestions. Initially, however, in the stepping towards the scenario, initial ethical questions are of focus in this article.

Autonomous vehicle (AV) deployment is highly anticipated due to its potential to ameliorate the world’s transportation system by mitigating road accidents, decongesting traffic, and reducing greenhouse gas footprints. To achieve its full operational effectiveness, AV is reliant upon vehicles capable of communicating with other road users in a production

environment(capable of environmental sensing, communication systems, and actuating vehicle functions based on sensor feedback) [2]. In particular, vehicular infrastructure can use the Internet of Things (IoT) sensor device for environment sensing, creating spatial perceptions to enable machine sensors on vehicles to 'see' the world around them, collecting essential data such as localization information, environmental images and data from connected services. Once an environment is perceived, IoT sensor-perceived data can be transmitted near- real-time to inter-vehicular, networked vehicles and transportation infrastructure, assisting a variety of autonomous vehicle functionalities [9]. Assumed fruits that AV can present include a safer environment on roadways, more-efficient traffic flows due to inter-vehicle communication, enhanced efficiency for hitherto manual processes such as parking and delivery service, and an Internet-connected public transportation infrastructure for voice control and artificial intelligence–assisted passenger interaction.

2.1. Definition and Functionality

According to the data requested in specific use cases [7], a high-performance and low-latency 5G network will guarantee seamless data flow, since formal measurements and specific criteria used for computer algorithms can be identified (i.e., the standard Mean Opinion Score scale). By leveraging a standard network, large sets of data with low latency values are collected from autonomous vehicles. Then, data are converted into standards that permit an easy collection of statistics about driver and vehicle behavior, which can be used to identify potential unwanted situations. Through the example of vehicles' data, we demonstrate the potential of AI ideas in creating functional computing methodologies that can play a relevant part in socially responsible usage scenarios. For this scenario, a connected and autonomous vehicle (CAV) demonstration was performed by assessing the 5G NR reference design, the PyTorch AI library, the 5G simulation platform netSim, and the connected eCall data tools. The geometrical representation and visualization of both driver state and vehicle status for different use events has permitted the validation of a concomitant and smarter use of the different algorithmic methodologies applied, so as to safeguard intervention, computing cost, and computing time.

In general, three frameworks can be identified as the key sandstone for the work in the IoT field: i) the 5C architecture, also well-known as the industrial perspective, conceived through the integration of computational cloud infrastructures, convergence of communication

technologies, and common protocols, ii) the N + N architecture, meaning the interaction between things and the interaction between things and humans, and iii) the dPMoS architecture, designed to optimize services (intelligent systems) without only considering the technological environment. In particular, in this scenario the current ecosystem is evaluated through the concept of "Digital Rights Management" by considering the physical context, the social responsibility, and ensuring the system security. The objective goals are to guarantee trustability and the security of things, disclose carbon-free hardware, ensure authentic data provenance, sustain privacy, and provide zero knowledge through block-chain technology [10]. This scenario helps to recognize which obstacles should be surpassed to reach stable collaboration in digitalization and transportation.

2.2. Types of IoT Sensors Used

In-cabin air quality, including the air for conditioning the vehicle's passenger compartment, is detected by air quality sensors mostly employed for ventilation control. Gas sensors have been designed in the 2000s for NOx detection: the infrared spectroscopy and the electrochemical methods built the base for the technological development for NOx detection. Nowadays semiconducting metal oxides are widely used for VOCs' in-cabin air monitoring by means of gas sensors. Among the most monitored ions in the in-cabin environment there are CO2 and CO, and specific sensors have been developed for both of them. Other materials used to build gas sensors are graphene, polymers, single-walled carbon nanotubes (CNTs), and metal carbides [11]. Different approaches lead to exhaust gases monitoring: from the use of infrared photometric sensors to the most sophisticated ones that include complex algorithms to transform inputs in meaningful values. The only type of sensor designed to offer a quantitative value of the air quality inside the cabin is the TGS 5141 sensor for measurement of total airborne volatile organic compounds (TVOC).

One of the main actors, if not the principal one, in IoT systems is represented by sensors. Sensors are devices able to manage and process information from the surrounding environment. They can transform information derived from the sensing of a certain physical or chemical quantity into electrical potential – voltage, current, frequency, or pulse trains – to be sent, managed, and interpreted by IoT devices [5]. They are of different types, depending on the quantity of interest. The most important sensors used in IoT systems can be grouped into three macro-areas: (a) sensors devoted to the detection of environmental parameters, (b)

sensors applied to the health status evaluation of human beings, and (c) technologies aiming at the detection of multiple subsignals. Many different environmental parameters can be monitored, however, only a subset has been historically monitored by means of sensors.

3. Ethical Frameworks and Principles in Technology Deployment

Technology is not immune to ethical concerns; rather, technological advancements present the risk of the unethical use of technical supremacy. Thus, it is critical to maintain a balance between expected advantages and potential pitfalls to ensure safe and just usage of technology for public welfare [2]. The deployment of radar sensors for AVs raises an important question concerning the requirements of sensors in unfamiliar environments. Traditional techniques for object detection, like monocular vision and radar sensor, may result in uncertain measurements, causing severe accidents. To safeguard autonomous vehicles from these uncertainties, diverse source sensors and advanced perception models are suggested. At the same time, from an ethical perspective, the deployment of IoT sensors in public or private zones should not feel invasive to individuals. Thus, a suitable anonymization technique is placed at the heart of the analysis for data collection and label generation for the AV scenario.

While technological advancements have played a crucial role in resolving emerging issues in our everyday lives, the deployment of novel technologies may have unforeseen impacts on society. Ethical considerations question the use of IoT technology in private and public spheres [12]. Thus, maintaining safety and security in uncertain environments has become a critical issue in the deployment of IoT-based sensors for monitoring AVs. To address such ethical concerns, this section studies different ethical considerations and provides a suitable framework for dealing with uncertain av environments.

3.1. Key Ethical Principles

[2] [1]Autonomous vehicles are electromechanical systems that use electronic devices and sensors to perceive and interact with the environment around them. The capability of the autonomous vehicle to perceive and interact with its environment is mainly attributed to Internet of Things (IoT) sensors, which can be located both inside and outside the autonomous vehicle. To ensure the correct monitoring of the status of a specific component of the autonomous vehicle by a specific sensor, the sensor itself should be properly located and

pointed toward the monitored component, in such a way as to include it in its detection range. Then, there is a need for exploring and defining a clear and comprehensive interaction model that investigates how sensors in autonomous vehicles can be used to monitor them, potentially using different 3D georeference system, data transmission protocols, and interaction paradigms with different infrastructural supporting elements. Long-term, autonomous vehicles that will need less space as consequence of the adaptive nature of the monitoring algorithms that, for minimizing the chance to lose their monitored component, dynamically adapt locally the sampling rate of their sensors and can stop the vehicle independently in a safe area, based on the monitored components and the transportation priorities.[8]Different aspects of the deployment of the IoT sensors and installed on roads for the real-time monitoring of autonomous vehicles are presented. To fully understand the ethical concerns related to the deployment of the IoT sensor on roads, many dimensions must be analyzed. First, the limits of the speed of autonomous vehicles must be strictly respected in order to minimize the severity of the accidents. The ethical implications of these constraints are discussed and a combination of statistical analysis, enhanced electromagnetic simulation, and nature-inspired machine learning is used for the optimal real-time management of drastic changes of speed, such as when a human operator brakes to avoid a crash. In recent years, road accident prevention systems have become prospective in countries with high rates of road accidents. The accuracy and reliability of these solutions have been improved by combining historical data on road accidents with real-time and road sensors. This article proposes a method for assessing the preventive impact of orthophoto maps, and the associated sensors in the field of road safety.

3.2. Relevant Ethical Frameworks

The context of the points made to this point is at a high level; the implications at the micro, meso and macro level are important. From a deontological point of view, for example, most people would consider it unethical to kill people, not only because it would involve a large disutility, but because it prohibits certain types of actions. In a goal to reach the 'good life' tons of action with bad consequences can be evaluated to be ethically good.,. Another large section discussed is if there is something good about good actions. This is called virtue theory and a virtue is a type of personal habit that is closer to a disposition to act in a certain (good) way. Furthermore, a kind of rule-oriented virtue ethics that can be seen as an intermediate point on the continuum virtues > rules > consequences (utilitarianism) can number the ends

among a few types of virtuous characteristic: it can be a balanced and socially responsible kind of rule-following, including following avoiding politicians and educators; might involve a certain kind of caring or strong friendships. Utilitarianism has a specific context of higher-level consequences, economics of consequence harvesting or geographical geographical the boundaries within which principals are to be judged.

This section discusses a number of ethical principles that could be relevant to the deployment of IoT sensors for autonomous vehicle monitoring. The aim is to provide a high-level overview of different ethical frameworks and it is not within the scope of this paper to go into details of the individual theories. There are multiple ways of categorizing ethical frameworks, and this section takes a pragmatic approach by discussing some specific frameworks relevant to IoT technologies. The discussion starts by considering consequentialism and some different classes of theories built upon this fundamental theory, including utilitarianism, egalitarianism and prioritarianism. The section also discusses deontological ethics, virtue ethics and pragmatic approaches to ethical questions. Members of the 'ethical operating system' for IoT run from simple rule-based approaches to more complex and contextualised implementations. This high-level characterisation defines the different murder rates, whilst leaving open whether they in fact translate into different levels of welfare at different values of the p_i. Additionally, the extra-legal and legally (or industry-level) regulated ethical standards are seen as constraint-based rule ethics [5]. In an extension to regulatory technologies, multiple pragmatic considerations are relevant, e.g. the extent of user-engagement found in the system/ technology, compliance with regulatory burden, as well as cost efficiency. Using utilitarianism as a base makes the system ethically tied to quantifiable welfare. This utilitarian solution might now be acceptable, or it might not. Depending on additional ethical side-constraints, the ethical implications can still be desirable or undesirable [6].

4. Challenges and Risks in IoT Sensor Deployment for Autonomous Vehicles

A related problem is the kind of objects that the perception system recognizes. To provide this information to learn its behavior, we perform detection and tracking on different sensor data such as camera, lidar and radar. Here, it is investigated that the sensor data having how many of the same objects in common and how efficient the perception system in object recognition. This part is the "data-in-tenor-sensor-modality" problem. An additional challenge in

producing the perception dataset for AVs ***system performance in complex environments*** the requirement of manually annotating the objects and input objects, because annotation is a process that needs remarkable effort, time, and proficient workforce. It is crucial to assert the importance of the shared perception dataset, hence we should eve prior information about the potential mistakes before reasoning about the performance.

An emerging and efficient prospect in the transportation industry is the trend towards moving from petrol or gas-based engines to fully electric vehicles. Along with this trend, there are other interesting concepts such as self-driven vehicles, advanced driver assistance systems, Internet of Things (IoT), and Collaborative Intelligent Transportation Systems (C-ITS) [13]. IoT sensor devices are used to collect information from the environment and turns it into conveniently usable data. The field of Autonomous Vehicles (AV) can make use of the collected data from the environmental sensors and estimation sensors to recognize and identify objects such as pedestrians, animals, and other vehicles on the road. Additionally, information from the environment can be used for improving the localization system of the vehicle. The performance of the autonomous vehicles that make use of algorithms for object recognition in a particular environment is subset of the data collected by environmental sensors. The data used to understand the environmental situation generally consists of data obtained from radars and lidar sensor systems. This data enables the vehicle to decide to act according to what information it gathered. The first problem is the number-of-object-detection problem. How many objects are observed in the data and how effective is the perception? A solution to this challenge may include collaborations among vendors and open-sourcing the perception datasets.

4.1. Privacy Concerns

The potential to use connected AVs' IoT sensors to collect data relevant to traffic incident monitoring raises numerous ethical and legal concerns, including questions of consent, data autonomy and self-sovereignty. The recent UK Centre for Data Ethics and Innovation has therefore highlighted the need for an ethical audit of the system which aims to put citizens in control of their transport and smart city data–especially given that a desire for social trust is emerging as one of the primary non-functional requirements for the wider adoption of connected and autonomous vehicles [2]. In this way, open questions around how to determine ethical thresholds for the use of AI and its decision-making remain. When implemented

responsibly, widespread adoption of connected and autonomous vehicle (CAV) systems and IoT technology could contribute significant, net-positive societal value and bring about greater public good. Though most current attention and resources are naturally focused on this most immediate and deadly threat, an attack against the human vulnerability inside a vehicle could also have drastic consequences and the development of IoT is far from secure.

[14] Autonomous vehicles (AVs) are essentially connected computers on wheels and they are reliant on the connections to the wider ecosystem known as the internet of things (IoT). Humans as part of the transportation ecosystem, and society in general, need to decide how to navigate the balance between the inevitable privacy trade-offs and the public interest in the deployment of IoT sensors in these vehicles without slowing down their adoption. Efforts to bridge this gap should address the following concerns in relation to the deployment of IoT sensors in AVs [15]: (1) autonomy, accountability, explainability, trustworthiness; (2) fairness, distribution, economic justice and equality; (3) security, safety, liability and traceable responsibility; and (4) privacy, transparency, data management as well as science-based policies and regulations. While these principles build on the conventional tenets of responsible AI and systems design, the deployment of advanced sensors in public spaces with concerns for private transport inevitably raises new policy challenges.

4.2. Data Security Risks

If we brake down the deployments of autonomous vehicle monitoring solutions to a high level architecture one can recognize that it is commonly built out of end-devices, gateways, a network and a service layer. From the service consumer perspective it is important to secure the service layer in order to ensure the users of the provided services themselves. For this consideration we have compiled a list of security and privacy risks that arise in such a deployment. These risks are discussed in the following subsections according to the layers of the shown high level architecture. Note that these risks are neither limited to the example implementation that we use as case (Parkopedia); nor can they be generalised to other specific settings (such as other IoT technology.).

Autonomous vehicle monitoring solutions are based on the combination of various IoT technologies such as sensors, edge, fog, and cloud computing resources, data processing (streaming, batching, analytics), storage and communication. This section explores some of the security and risk considerations that appear in providing such services over commonly

used IoT technologies in the automotive industry. [2] [16]. Developers of urban-scale IoT technologies have to cooperate with a multiplicity of stakeholders, who have different, and often conflicting, interests and ethical considerations [8]. For instance, while participating in our case study, within Parkopedia, we realized that city-based services (such as on-street parking availability and autonomous vehicle monitoring- the case study technology) have a significant impact on the interests of local city councils and community residents. On one hand, city councils and citizens always request maximally precise and real-time data (e.g. to optimize the performance of a city's parking management and urban environment).

5. Case Studies and Examples

With appropriate protection of the personal data and if the driver has given consent for using the side camera for registration, it would be possible to use the camera for monitoring the health state of the passengers literally on the go (Gorne, 2019). As parking already in 2020 has become an activity for standing approximately 10% of the time, there would be quite a number of passengers to follow the health state among, but less complexed challenges concerning privacy. However, the privacy challenges would arise when sharing these health data with, for example, an emergency center, emergency vehicle, and others. Another study foresees even influencer tourists to be followed on the go by sensors (Bretschneider et al., 2015). In this study the participants are considered as being influencers, and using sensors to also follow their health is considered an added service they provide when traveling. By defining two types of ethical and privacy protection innovations aiming at different groups (citizens and influencers, respectively), thereby taking different social-economic roles into account, a new ethical and privacy protection challenge is foreseen. Goals to strive for include that emerging technologies should have some embedded trust and the necessary transparency and that practical acceptance should not be the only ethical evaluative criteria" which is traditionally claimed for analogue and digital media. Just because it can be done, it is not always desirable or permissible.

[17]The Ciudad 2020 project (Bench-Capon et al., 2020) proposed the development of a public parking control system. Using off-the-shelf IoT elements, monitors the parking of vehicles in smart cities. Here our concern is the privacy of the passengers in the vehicles. Apart from observing the parking itself, the camera—on the same side as the parked car—can record the registration plate and the person if the side window is open. Assuming the number plate is

protected in a way that the raw data are processed locally in the vehicle and not broadcasted, the ethical challenges for privacy presume we have enabled appropriate access control to accessing and protecting those data in the vehicle.

5.1. Real-world Deployments

Consideration of ethical issues in the realisations of IoT-based autonomous vehicle operations while monitoring their operational status for actual deployments has a significant contribution to operational efficiency, safety, environmental sustainability, and is a major agile treatment for road-based operational marginalisation. Taking into account to large-scale pilot for ethical technology deployment, the deployment of intelligent IoT sensors in autonomous cars for traffic data analysis and sharing contributes to the efficiency and effectiveness of the developed and implemented technology. The sharing of traffic information obtained by IoT sensors through VANET provides the vehicle operators with accurate insights and guidance for vehicular ahead operational conditions [12]. Therefore, the ethically grounded solution that fosters the integration of advanced intelligent transport solutions to transpire into effective practices is the IoT-based operational monitoring used in the intelligent autonomous or connected vehicles by exchanging information via VANET to improve traffic regulation and control.

There are many ideations of ethical consideration in the deployment of IoT sensors for monitoring and valuation of real-world deployment of IoT sensors. Vehicular ad-hoc networks (VANETs) are the means by which autonomous vehicles can assess and exchange data in the network. Although VANETs are regarded as a secure and reliable communication network, the VANET network environment is open, which makes it susceptible to safety and security issues caused by intruders, attackers, and disasters that deploy IoT-based VANET sensor technologies for traffic operational status monitoring applications [2]. For the deployment of traffic operation monitoring sensors and actuators, the major contributor for ethics is security assurance for the related communication systems to tolerate illegal message tempering as undependable message transmission on VANET can affect operational statistics.

5.2. Ethical Dilemmas and Solutions

Public health monitoring, which targets only the driver, could be totally separated from non-public monitoring by default, and therefore address some of the privacy concerns of drivers,

passengers, and other road users. However, non-public health monitoring allows some targeted advertising with the potential, using high-frequency physiological sensing, to even identify people. Algorithms examining the biosignals must also restrict the transmission of any biometrically identifiable information to other on-board devices or remote nodes. This solution implements the pseudonymization and data minimization rights by design, but must ensure that the healthcare provider of the monitoring service remains legally fully responsible, ensuring that any health decision reuse of monitoring data respects the subject's privacy after user consent. Such a healthcare provider would also ensure transparent redress mechanisms when something goes wrong [18].

To minimize ethical dilemmas in deploying IoT sensors for autonomous vehicle health monitoring, there needs to be early discussion of how serious privacy intrusions can be avoided while preserving the potential benefits of the technology [11]. We propose two solutions, for public and private health monitoring, which separate physiological recordings from the arbitrary communication of sensed data. Standardized terminology and general ethical guidelines are provided in the article to minimize research duplication and ensure responsible research sharing.

6. Regulatory and Legal Considerations

The so-called trolley problem has become a paradigmatic case of an ethical challenge in machine ethics widely discussed in railway, aviation industries, and now also in autonomous vehicles [2]. A vehicle cannot make such decisions, because the decision concerning the permissible range of collision with others constitutes the core of traffic law and court-administered argument. An algorithm might not "see" a dog at zero points, and cannot recognize passengers hiding behind obstacles. In contrast to human drivers, a system will not make legal mistakes. Otherwise, it inspects complex traffic rules and their interpretations in each country and decides on its behavior based on all interactions with all participants.

The potential use of algorithms in an autonomous vehicle system places it within the concept of an Internet of Thing IOT devices [6]. Such algorithms can involve sensors from a complex array of devices such as laser scanners and cameras for environment perception, inertial sensors and odometry for vehicle self-localization, and global position sensors to obtain geolocation. We are faced with the ethical challenge to correctly and meaningfully embed such urban IoT capacities into the transport data infrastructure. With regard to the application of

algorithms to virtual sensors such as IoT and IOT-enabled algorithms, it is also necessary to observe that the concept of the observation of private space by some sensors, e.g., video sensors, could lead to an increased risk of cyber attacks or data manipulation [19].

6.1. Current Regulations

Criticisms of the current regulatory models for data privacy stem from the fact that they are not fit for the expectations of modern consumers. Identifying the European Union's GDPR policy as the most progressive legislation as it rights, a study of UK citizens found that a significant proportion of the sample did not believe that the law extended protection to the IoT. Similar criticism is leveled at the United States where privacy legislation is implemented on a state-by-state basis, rather than at a federal level, leaving regulation fragmented in much the same way as IoT data is. It is not just the physical storage and management of the data, but the events, people, and occurrences as a part of these decisions that need to be handled in line with data protection laws. These requirements inherently conflict with new business models and value chains, especially those that include data sharing. Taking a proactive stand in assuring the rights and autonomy of the individual, Atzori advocates that privacy should represent one of the foremost priorities of the IoT vision. Projects should invest in educating the general public on the use of their data and IoT and also emphasize digital identities that can individually authenticate and public keys which are stored either in a centralized repository or in a decentralized manner. Smaller projects may not have the resources to invest heavily in these areas and it should be enough to ensure that users have coherent information about how their privacy is protected, the efforts management is willing to make to ensure IoT data protection, and the risks to individual security both underhanded and informational, be those physical and in cyberspace.

One of the challenges surrounding the widespread use of the current IoT devices in both research and business contexts is the ambiguity surrounding data privacy regulations. The ambiguous nature of privacy regulation in business contexts is highlighted by the fact that with the exception of the Netherlands, regulations and legislation are vague regarding the data rights regarding IoT devices and the sharing of this data with third parties. Not only will commercial data sharing require individual user consent, but consent will also need to be explicitly and freely given. A notable achievement of the IoT device industry has been the EU's General Data Protection Regulation, which consolidates regulations across all 28

member states, providing individuals with the right to request information on the data process behind an automated decision, the scope of data processed, and ultimately, for the incorrect data to be rectified.

6.2. Proposed Legislation

Given that these two applications of autonomy are highly estimated, a huge market will appear for ethical technologies. It is only a matter of time until self-driving vehicles are on the road. The American potential disappointment holds a warning for German car manufacturers. Hitherto the other major international manufacturers did not have the slightest doubt that the future belongs to vehicles without a driver. They bet all their money on the assumption that more than 90% of all road traffic will go from person driving to the driverless pandemic. What now? We also know from research that trust in ethics parameters has a direct impact on customer acceptance—on the purchase willingness of automates. Here also, matters concerning goods and services have come to a head. The relationship between manufacturers and purchasers was never so intimate as with cars. Privacy had best be born in mind in the young industry. A solution must be found that makes the whole development transparent for end users in any case. Second, we see a need for improved telematics data aids, present already in all new cars. Concerning the legislation for the—hearable—surveillance, this mode should be disallowed in a private passenger car from the beginning. Nonetheless, we can predict that a lot of data obtained today can be included in the decentralized braking reserve of tomorrow.

'article_id': '020a994a-c5cc-4537-934c-94df0ef5058e' The timing is good, since the chart of 100 autonomous driving scenarios in Germany, a hot topic at the moment, reveals a different moral among drivers for each scenario. Besides, drivers are in accordance only to some extent with the general public. In other words, there are differing cultural approaches to the ethics of risk-taking cases if push comes to shove. The referees in EuroNCAP will certainly have a lot to do in the future. Penultimately, and this is a paradox, there is one more factor influencing the development of products as the service provider. According to the guidelines of the Federal Department of Traffic (Bundesverkerksamt, Leipzig, Germany), even if one can prove that an autonomous vehicle is collision friendly in all scenarios, the autonomous bus stipulated by the mid-market will not be approved. Here we go again. We have consent to kill—internationally. Ethical standards unfortunately refer to possible accidents, not to

possible cases where a group of people kills themselves. Nevertheless, a highly connected vehicle will be driven from 2018 onwards.

By 2035, 0 1 2 3 4 5 6 7 8 Ghost vehicle every new vehicle will be reading signs and acting upon them. In this legislative context, we are now developing the VW Car. Net in several directions to monitor ethics. The VW version equipped with telematics purports to determine the parameters of ethical consequences in risk-taking traffic decisions in known traffic constellations. The idea is to contemplate ever more scenarios deemed relevant by the public. In addition, the development focuses on various drivers, having already driven the VW brand before the law was enacted. These drivers already have a tacit knowledge of what is allowed with a VW model. Our Car. Net will put the driver's adaptive behavior in numbers. Last, two additional interfaces are planned in the telematics. The car's module reads the driver's intention. This mode is needed by insurance. A further interface will show good driving.

The above requirement that the vehicle must be covered by insurance was the starting point; however, the regulation did not stop there. In 2016, connectivity for newly registered light vehicles and trucks will be mandatory within the EU. The officials deliberately did not mention a technical solution; rather, preferred technologies are Ethernet and Wi-Fi. The European Union also stipulates that in 2018, e-Call, an emergency call, will be obligatory for all new vehicles introduced in the European Market, which will comment HARMAN, 2011 with telematics bus Missing annotation: it. The tele- matics bus, often known as a passenger compartment bus, is an in-vehicle data bus and a network which allows vehicle devices to communicate with one another. All of this means the law is now gearing toward autonomy and thus preparing the market for technology such as offered by TC2 in the years to come. It is not unlikely that the EU will set further more demanding standards.

7. Stakeholder Perspectives and Engagement

Unfortunately, the research that is currently needed to build a clear understanding of these issues and concerns is lacking, mostly due to the early stages that this technical domain of AVs and IoT is currently in. Finding and discussing potential stakeholders is, therefore, important in being able to connect with these stakeholders, gauge their needs, and collectively come up with ideas for research topics. This type of work is still in its infancy. It is, however, fundamental to future development of IoT sensor technology for AVs. In this chapter, for the first time, we introduce stakeholders in the IoT Devices domain and discuss the possible

perspectives they might hold to open the door to future collaborative research. The perspectives discussed are important because understanding the complex motivations and requirements of these diverse stakeholders will lead to more socially impactful research [6].

Many autonomous vehicles (AVs) are now equipped with intelligent transportation system sensors, including integrated technologies from mobile and internet of things (e.g., IoT) devices. The origination of a vast number (and new types) of intelligent infrastructure devices that can be used for real-time data collection has generated ethical and social considerations in the last few years pertaining to the use of these resources and how they will interrelate with citizens and their data. It is, therefore, of increasing importance to understand potential social and ethical issues in this domain to ensure citizens are not adversely impacted and to be able to continue to develop these devices collaboratively and constructively. As such, government bodies, industries, and researchers now are needing to comprehend, engage, and manage people and communities in which these devices are encroaching. This chapter aims to identify possible stakeholders in the deployment of IoT sensors for monitoring in an autonomous vehicle environment [1].

7.1. Industry Perspectives

Introducing AI into automotive systems raises important ethical concerns in the form of cyberphysical systems (CPS) that consist of collecting, processing, sharing, and act- ing based on sensor-generated data. This work navigates this critical interdisciplinary research area by not limiting ethical considerations to sensors/ hardware or humans/vehicles, but rather focusing on software, methods and tech- niques conveying data and knowledge back and forth between humans and autonomous decision-making processes. Industry stakeholders, service providers, end-users, society, and politicians have been focused in this study on their role in autonomous systems' statistical transparency, model conservatism, data minimization, accountability, and verification, partly by data ethics principles research. In different phases of a vehicle's life cycle, the Vehicle Retail Industry generates the raw data for different stakeholders such as Consumers, Original Equipment Manufacturers, and other third-party vendors. Industrially, the International Organization for Standardization has been devel- oping standards around explainability in artificial intelligence. An accompanying working standard explains xAI focusing on languages, protocols, and interfaces, mechanisms, and models from revision C in JCGM/WG 7. Open Reviews of Modern Physics is an interesting

case of AI applied to peer review by extracting, through advanced text mining with aggregated nanopub- lished data, the marginal benefit of opening peer reviews to scientific users [8].

Providing an ethical framework and associated technologies relevant for the deployment of IoT (Internet of Things) sensors for autonomous vehicle monitoring, especially for the data from such sensors that is transmitted to and remains on the cloud without direct access by the vehicle operators. Solutions for deploying smart sensors in self-driving vehicles must be practical, accurate and cost-effective—this may involve multiple sensors such as Lidar, and especially when the vehicle is not driving in the full self-driving mode, the additional cost could be avoided. For example, in Lidar devices, single LIDARs with wide field of view have been proven to be effective to solve the sensor placements without relying solely on the IMU and GPS sensor inputs, especially for drift and sensor noise countermeasure. In general, a variety of sensor technologies are being developed and experimented with that are powerful enough to withstand the major traffic conditions in crowded mainland cities in Asia with the ability of obstacle detection at a long range, nighttime, and in dense fog, but also are working in combination with a minimum of developed sensor NCAPs. Despite Lidar, other car sensor technologies such as IMUs, or alternative braking systems, such as direct drive braking/driving systems for electric vehicles could also be used instead by smartphones as a vehicle access key.

7.2. Public Perception

According to the IHS automotive estimates in 10 to 15 years, approximately 60% of new cars sold will be connected vehicles. An intelligent transportation systems (ITS) continuously specialized the landscape with the addition of new interoperable features that provides facilities not only for the traveling citizens but also for organizations and government bodies. According to the authors, the networked Intelligent transportation system (ITS) emerged as Internet of Things (IoT) and the connected vehicle technology has revolutionized the operation of the ITS, encouraged the development of cooperative mechanisms and services, and helped in meeting traffic and safety management goals of transportation authorizes. Real-time information exchange of vehicle-to-vehicle (V2V), vehicle-to-traffic infrastructure (V2I) and vehicle-to-network (V2N) is considered as Co-operative-ITS functionality [20]. Innovative and outstanding research activities aim at the significantly improving and establishing better

and superior co- operative ITS. Scientific effort is invested to solve technical, societal, and technological issues. Many issues regarding user identification, reliability and authentication, anonymization, the payment and billing procedures for V2N, V2V and V2I communications are being solved with a lot of difficulties.

Public perception and public attitudes are important areas to study, as negative public perception toward the successful deployment of ADAS/RSDSS can have negative impact on Acceptance and Usability [21]. It is important for society to realize the importance of new road safety and to safeguard the privacy of drivers and passengers at the same time. The authors have presented the ethical perception and social acceptance of Autonomous and Connected Vehicles (ACV) with the following objectives: moral aspects of ethics and road safety in smart, connected and autonomous vehicles, analysis of public perception and ethical considerations in information security, and the social perception and effect on social acceptance [22]. The author would like to slice the ethical considerations tied to public perception, user acceptability, security and privacy of Connected and Autonomous Vehicles in future research works. For correct operation with the external environment, the perception by sensors of the environment must be associated with a map of the region in which the vehicle moves, ensuring the security, the data legitimacy and avoiding problems of theft.

8. Future Directions and Recommendations

Overall, the previously mentioned issues are relatively known and have already been successfully addressed by industry in other fields such as standardization in the telecommunications industry. The regulations that will need to be put into place in the field of VIoT are similar and will likely one day allow for millions and billions of social vehicles to drive safely in our cities without the need for any extra ethical regulation. With the technologies and developments that continue to interact and increase with vehicles, we have to continue surpassing artificial intelligence that is continuously learning from data. It is possible that the best potential technology that can be developed may not at first glance appear to be as respectable. The biggest todos at the present time are therefore lacking an advanced theoretical framework backed by real global must-haves and specifications for cars moving independent of people while trying to solve some kind of rule violation error [11].

[20] A key element of improving the ethical considerations of vehicle monitoring is the ability to accurately and successfully analyze the information from the sensors and have this type of

information made available and available to use by all participating members. Accordingly, there are several measures and strategies that may be deployed to address some of the potential areas for ethical concerns as outlined in the previous section. Some of these strategies are generalized specifications, and guidelines that should be developed for a point in time when the number of globally deployed vehicles that can interact continues to increase exponentially. Another existing dilemma that may require regulatory/committee action or regulation updates is to determine which entities on the roadways are able to act as potential unethical sirens capable of exploiting vehicles with access to the networks of data exchanged.

8.1. Ethical Guidelines for IoT Sensor Deployment

Compliance with legal provisions and ethical consideration must be considered in the design of an IoT system to avoid potential challenges, including privacy intrusion and autonomy infringement. We cannot assume that there will be no disputes with the ethics and privacy of IoT data in car-centered monitoring projects that use an IoT to determine the cause and effect of autonomous traffic accidents [8]. To mitigate this problem, we proposed and summarized ethical considerations to be thought through in the initial deployment of an IoT sensor network to be used for autonomous vehicle monitoring. These considerations will help guide the stakeholders in navigating the novel ethical issues that arise when the IoT is used for the structuring of an automated system, and will help to shed some preliminary light on the crucial dilemmas faced by technicians today.

For better results, autonomous vehicles (AVs) should harness the power of the IoT to improve safety and promote open innovation. Yet, we need to consider the caveat that AVs cannot share data too extensively. From a purely practical stance, there are already security and safety concerns that arise from so much digital information being collected and shared—so much so, in fact, that these are now being referred to as the dual "sociotechnical" perils of AVs. From an ethical/commercial standpoint, if the IoT products can curtail the amount of data they allow AVs to share, then it will be more difficult for the AVs to achieve their promise of safety, which is, after all, a big part of the main selling point of an AV [15].

9. Conclusion

The results reported in this paper suggest that: safety is the prime concern for frequent exposure to automated vehicles, the public has a limited understanding of the sensors, engine,

learning and decision processes of autonomous vehicles, the prime driver in the future would need to be able to take over in an immediate emergency situation, expanded public and drivers' understanding of the alert and panic triggers of the autonomous vehicle and addressing public safety is a top priority over company personal and company ethics. This was supported by the public respondents reporting perceived safety to be the highest causal factor of formal authority transfer. The results of this study indicate that the initial response to new technologies such as HMIs for formal authority transfer in autonomous vehicles is often driven by the priorities and climate of the time. This respondency, the ability to quickly adapt, and the context of self and mood is important to project as every company has different technologies with different facets to public and driver response times. New technologies such as augmented reality and virtual reality versus the current models shipped by Google, Uber, etc. are an area of great interest. Robustness — the sensitivity to change in inputs (data or conditions) — is tied to the reliability of an AI model, which affects its cost, time of development, generalisability in different environments, and vulnerability to adversarial attacks which this paper has attempted to factor and present.

[23] This paper explored the ethical aspects, issues, and concerns surrounding the integration of autonomous vehicles with IoT connected infrastructure to enhance public confidence in the investment [24]. Autonomous vehicles are the focal point of automotive research and development efforts which are focused on full autonomy and accident-free driving. The underlying belief is that traffic collisions are inevitable but the issue of "who is in the driver seat" during potential injury or traffic collisions is unresolved and may present a substantial challenge to the wide-spread deployment in the near future. In the absence of trust, the general public and consumer acceptance of highly autonomous vehicles would be low. It is therefore crucial that all aspects of safety associated with the future autonomous vehicle roadmap are thoroughly investigated (e. important cybersecurity risk, infrastructure readiness, driver's behaviour, all weather scenarios, wheel and brake standardization, Vision anomalies, attack delayed response, AI systems, onboard/offline implications, GNSS level coverage, wireless channel capacity and 5G vehicle-to-vehicle and vehicle-to-infrastructure standardization) [15].

9.1. Summary of Key Findings

A risk assessment outlines the main ethical issues going from the sensitivities of each potential stakeholder (and potential ways of at least partially addressing the issues that are ethical related), and thus the potential threats for each potential "adversary" to the system as well as for other stakeholders. This helps to provide a comprehensive understanding of vehicles connected to monitoring applications related to CVs, research questions are drawn from the main ethical issues encountered in the literature, even if the contribution is not observed in practice. The research questions can be useful for discussing the ethical issues of every ECA and provide some solutions to mitigate the problems [8].

Ethical considerations are important as we transition from traditional connected vehicles to autonomous vehicles. Autonomous vehicles with IoT-based CV monitoring applications demand a trust boundary between the participant vehicles and the stakeholders (roads, authorities, service providers). This section aims at providing a list of core ethical issues and the difficulties posed by the current self-interested approach that preclude an adequate practical guidance in the deployment of sensor technologies [6]. The goal is to understand current approaches in general and to explain what is currently missing, leaving developers and managers without adequate ethical guidance.

9.2. Implications and Recommendations for Practice

Special ethical concerns overuse of genealogy databases for genetic genealogy and isnôt the general concern of data privacy but rather a concern about unwanted identifica- tion. Thus, related industries take privacy and ethical concerns into consideration. The primary ethical concern recognized when deploying IoT sensors for monitoring autonomous vehicles under the Inform and Inquiry Ethical Policy is unfair use. In order to avoid or mitigate the ethical concern, it is recommended that impact of IoT sensors for autonomous vehicle monitoring should be included in the local policies of the municipalities New York City. In efforts such as the private and secure mobility partnership in New York City are established and followed with R&D work that involve in-situ research w.r.t.law enforcement. The 'Data Integrity' layer is aimed at achieving privacy and confidentiality of data before it is collected and transmitted to data mechanisms when appropriate [6].

Multiple cybersecurity standards and privacy-enhancing techniques can compensate for the malicious means of privacy intrusion by creating a secure and private environment. In particular, the most important privacy protection for IoT, such as autonomous vehicles, is

brought by privacy enhancing technologies and efforts to fully comply with data minimisation and purpose limitation in data processing. Pseudonymisation and pseudonymous data processing as the alternative to the processing of personal data in IoT have gained significance in this regard. Efficient slutions are proposed by multitudes of researchers that would cure this weakness by PR technology [10]. Also, efforts should be spent to practice data minimization and purpose limitation in IoT data processing. Among challenges encountered when minimizing data communication prop- erties in vehicular communication systems, the loss of requesttraceability has been used to illustrate one of the problems that appear when minimizingvedata communication. It is also shown that by using cryptographic primitives in anonymous credential systems, such as the collective verification signaturecertificate or the zero- knowledge argument, it is possible to identify malicious Pseudonyms by verifying trusted certificates [8].

Reference:

1. Pulimamidi, Rahul. "Emerging Technological Trends for Enhancing Healthcare Access in Remote Areas." *Journal of Science & Technology* 2.4 (2021): 53-62.
2. Tatineni, Sumanth, and Venkat Raviteja Boppana. "AI-Powered DevOps and MLOps Frameworks: Enhancing Collaboration, Automation, and Scalability in Machine Learning Pipelines." *Journal of Artificial Intelligence Research and Applications* 1.2 (2021): 58-88.
3. Ponnusamy, Sivakumar, and Dinesh Eswararaj. "Navigating the Modernization of Legacy Applications and Data: Effective Strategies and Best Practices." Asian Journal of Research in Computer Science 16.4 (2023): 239-256.
4. Shahane, Vishal. "Investigating the Efficacy of Machine Learning Models for Automated Failure Detection and Root Cause Analysis in Cloud Service Infrastructure." *African Journal of Artificial Intelligence and Sustainable Development*2.2 (2022): 26-51.
5. Muthusubramanian, Muthukrishnan, and Jawaharbabu Jeyaraman. "Data Engineering Innovations: Exploring the Intersection with Cloud Computing, Machine Learning, and AI." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 1.1 (2023): 76-84.

6. Tillu, Ravish, Bhargav Kumar Konidena, and Vathsala Periyasamy. "Navigating Regulatory Complexity: Leveraging AI/ML for Accurate Reporting." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 149-166.
7. Sharma, Kapil Kumar, Manish Tomar, and Anish Tadimarri. "AI-driven marketing: Transforming sales processes for success in the digital age." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.2 (2023): 250-260.
8. Abouelyazid, Mahmoud. "Natural Language Processing for Automated Customer Support in E-Commerce: Advanced Techniques for Intent Recognition and Response Generation." *Journal of AI-Assisted Scientific Discovery* 2.1 (2022): 195-232.
9. Prabhod, Kummaragunta Joel. "Utilizing Foundation Models and Reinforcement Learning for Intelligent Robotics: Enhancing Autonomous Task Performance in Dynamic Environments." *Journal of Artificial Intelligence Research* 2.2 (2022): 1-20.
10. Tatineni, Sumanth, and Anirudh Mustyala. "AI-Powered Automation in DevOps for Intelligent Release Management: Techniques for Reducing Deployment Failures and Improving Software Quality." Advances in Deep Learning Techniques 1.1 (2021): 74-110.