INDIVIDUAL TERM PAPER:

"PRIVACY ISSUES IN AUTONOMOUS VEHICLES."

CSCI 5001: PRIVACY & IT

PROF. CARLA HEGGIE, BA, IAPP(Alberta), CIAPP(M)
INSTRUCTOR & FACULTY OF COMPUTER SCIENCE

AUTHOR OF PAPER: RUHI RAJNISH TYAGI
AFFILIATION WITH: DALHOUSIE UNIVERSITY
FACULTY: COMPUTER SCIENCE
CITY & COUNTRY: HALIFAX, CANADA
EMAIL ADDRESS: ruhi.tyagi@dal.ca
BANNER ID: B00872269

The era of autonomous automobiles is rapidly approaching; it is no longer science fiction. Without a doubt, self-driving cars are already beginning to transform the auto business. In the era of highly automated data collection made feasible by big data techniques, artificial intelligence-powered personal identification algorithms, and perhaps millions of sensor-rich autonomous vehicles, privacy risks are significant. Autonomous driving systems are able to collect a significant amount of data while in operation due to the broad and diverse array of sensors they use. The Society of Automotive Engineers International (SAE) guidelines for levels of driving automation in autonomous vehicles (AVs) are referred to in numerous laws in Canada and other countries. In Canada, British Columbia and Alberta have SAE level 3,4, and 5 autonomous vehicles in Pilot phase, Ontario and Quebec have in level 4 and 5 while Nova Scotia has level 3 still in pending state. There are not enough automated tools to perform a privacy audit. If a possible threat is indeed a privacy concern, it is required for developers to examine the relevant code segments. In this essay, numerous privacy concerns will be covered, along with their effects on people's lives and potential remedies. These concerns will vary depending on how data is acquired, processed, and/or disclosed. Where applicable, it will also discuss about Privacy by Design, the parts of Fair Information Principles and/or legislation bills in connection to autonomous vehicles.

Location data, such as destination information, route information, speed, and duration of travel, must be gathered and utilised in autonomous cars. In addition, location features are utilised in conventional automobiles to establish routing preferences, such as avoiding highways or toll roads, and to deliver additional trip-related information, such as real-time traffic reports and areas of interest along the planned route. Given that it can also collect extremely private information like the trip to a union meeting, plastic surgeon's office, gay bar, AIDS treatment facility, criminal defence lawyer, by-the-hour motel, and abortion clinic it can reveal the preferences and travel patterns of a person. This may increase the possibility of physical violence or stalking if the wrong people obtain that information. In general, personal information may only be collected, used, and disclosed in Canada for "purposes that a reasonable person would consider to be acceptable in the circumstances”[1]. Therefore, meaningful consent processes should consider the viewpoint of the consumer to make sure that they are user-friendly and that the information presented is generally comprehensible from the point of view of the organization's target audience.

Autonomous vehicles may collect and store identifiable information as private as iris scans or facial arrays of the owner or passenger of the vehicle for a variety of reasons, such as to validate permitted use or to customise comfort, safety, and entertainment settings [2]. Owners, passengers, and their actions may potentially be recognised with remarkable accuracy using this data. Such information may be used, altered, or sold to third parties without the users' knowledge. Biometric databases being a possible target for hackers and putting consumers at danger of identity-based assaults is another issue. They might be left with no choices if this happens. A password can be changed, but fingerprints and eyes cannot be. Apart from this kind of primary data, autonomous vehicles collect secondary data which is not a unique identifier, but it can be merged or linked with other information to re-identify persons. Driving patterns, environmental

information, and the gender of the driver or passenger are some examples of secondary data. In response to these problem, people should be given explicit options to say "yes" or "no" when giving consent, as well as actual choices for controlling how personal information is handled, such as the ability to turn off specific sensors or ask that certain user records be deleted.

Regarding a more specific area of data gathering, there are locations inside the automobile where users' explicit personal information may be obtained without their knowledge [3]. For instance, the dash cameras' visual data reveals the identity of the users (the driver and passengers) by their facial characteristics when they are inside the car. The attacker can discover the behaviour of the driver and passengers as well as other private information about the users by looking at the photographs and videos at a particular time. Additionally, the dash camera may record the display of a smart device being used inside the car, such as a smartphone, smartwatch, or computer. This will cause any messages, alerts, or entertainment items to be revealed on the screen. Since the system software that controls the entire autonomous vehicle has poor privacy protection, hackers can implicitly access any vehicle and direct its movements without the owner's knowledge by exploiting this software. Hackers may specifically target the vehicle's controller system, causing disruptions to the vehicle's speed, route, and braking system. In such case, information collected like this should be deleted after a certain interval of time where it is no longer necessary to be kept as it might not have any use that driver has consented to collect, use or disclose which is one of the principles of fair information.

In vehicle-to-vehicle (V2V) networks, AVs broadcast information to neighbouring vehicles about road dangers, traffic congestion, and speed, location, and movement intentions [2]. Such data is necessary to improve driving safety, prevent collisions, and recalculate routes. Due to the anonymity of the vehicles on the road and the uncertainty of how the given data will be used by another vehicle, data sharing among vehicles raises major privacy concerns. The vehicle's photos can be captured from the side or close to it by AV sensors because they are able to sense their surroundings. These photographs could include information about the car as well as the visual data of the driver and passengers (model, colour, and speed). Furthermore, if the vehicle is frequently identified in a particular area or during a given time period, the opponent can launch a linkage attack with great precision on a target. User profiles and identities may be revealed as a result of unauthorised parties using such information improperly. Therefore, businesses collecting extensive amounts of data may want to put in place safeguards to preserve people's privacy. Anonymizing all of the information that self-driving cars gather could be one way to ensure privacy, for example by ensuring that particular travel plans or trip specifics aren't connected to a single person.

Vehicle On-Board Units (OBU) will communicate with static infrastructure and stationary objects on the road that have intelligent features, such as parking management systems, traffic control systems, CCTVs, toll plazas, smart buildings, and billboards, in vehicle-to-infrastructure (V2I) communication [3]. These systems will be outfitted with cutting-edge functions as IoT development continues to grow, allowing more data interchange among devices and exposing vehicle owners to new privacy

dangers. The reservation of parking is an illustration of communication between automobiles and infrastructure. Some programmes can gather information from an AV to handle parking spots, such as Bosch Automated Valet Parking. No two AVs will occupy the same area due to the cloud processing of all reservation requests. Therefore, here it poses risk to personal information and personally identifying information of the user collected, used and/or disclosed by third party (i.e. infrastructure) which users never consented to and have no idea whatsoever. In accordance with Canadian privacy laws, organisations are accountable for the personal information under their control, including information provided to third parties. According to the Privacy Commissioner, this requirement encompasses designing privacy protections into a product or service.

The autonomous vehicle's voice recognition and control system is one "sensor" that need special attention. Consumer electronics adopting this technology have raised concerns and grievances from the public over the transmission and collecting of private conversations. These components generally communicate with one another using proprietary protocols that are exceedingly challenging to maintain or integrate in autonomous vehicle systems. In many instances, the system makes the assumption that reliable resources are available to handle communication, queries, and computation for applications that are deployed and controlled in infrastructure or vehicles. Therefore, it is necessary to restrict the sharing of data produced by cars and other smart devices. This is due to the possibility that the vehicle's components came from several suppliers, some of which might not have complied with privacy protection laws.

Let’s consider a real-life scenarios where autonomous vehicles will have tremendous impact on an individual’s daily itineraries. Now the car has looked through your emails, noted important words, and evaluated similar communications for emotional tone, so it is aware of your preferences. There was that one time you raved about a certain product you had tried the night before to a friend who was riding along with you in the car. When the same product went on sale, the automobile heard your discussion, recognised brand-related terms, and suggested it for your shopping list. This is an enticing practice for customers and marketers but it puts so much of the user’s privacy on stake. As in the example above, the chats with a friend were not as private as they believed, and having the acquaintance inside the car was an obvious indicator that they wanted to speak in private, but the automobile just violated on the right to be left alone.

In conclusion, it may be said that autonomous vehicles inherently have the ability to limit or lessen personal autonomy. Surveillance is the price of convenience. People might not be able to make well-informed decisions regarding how their personal information is handled as a result of the complicated architecture of AVs. The enormous volume and diversity of data that these autonomous vehicles gather has more negative effects on customers than positive ones. The development of autonomous vehicles is anticipated to proceed quickly and has already generated a lot of interest, but prior to their commercialization, it is essential to carefully consider the risks and legal repercussions of collecting and using personal data as well as various cybersecurity issues. Autonomous vehicle companies should be aware that Canada is

currently going through a substantial phase of privacy regulation reform. Many Canadian provinces are currently updating their private sector privacy law frameworks due to developments in other countries, consumer , and political interests. Importantly, preliminary results point to the likelihood that these reform initiatives will bring AI systems inside the jurisdiction of private sector privacy regulations. Given that cars might traverse both national and provincial boundaries, AV companies that operate in Canada must consider how to abide by numerous privacy rules. But before any such changes take place, autonomous vehicles manufacturers need to abide by the rules like PIPEDA (Personal Information Protection and Electronic Documents Act) which governs all the private sector data collection strategies in Canada [1].

Total words: 1784

REFERENCES:

[1] "Personal Information Protection and Electronic Documents Act", *Laws-lois.justice.gc.ca*, 2022. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-2.html#h-6. [Accessed: 08- Jul- 2022]

[2] T. -H. Nguyen, T. G. Vu, H. -L. Tran and K. -S. Wong, "Emerging Privacy and Trust Issues for Autonomous Vehicle Systems," 2022 International Conference on Information Networking (ICOIN), 2022, pp. 52-57, doi: 10.1109/ICOIN53446.2022.9687196.

[3] M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah and W. Alasmary, "Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey," in IEEE Open Journal of the Communications Society, vol. 3, pp. 811-829, 2022, doi: 10.1109/OJCOMS.2022.3169500.