# IEEE DIGITAL PRIVACY MODEL: A PRIVACY FRAMEWORK FOR THE CONNECTED VEHICLE ECOSYSTEM

**Dave Michelson**
Department of Electrical and Computer Engineering, University of British Columbia

**Amith Khandakar**
Department of Electrical Engineering, College of Engineering, Qatar University, Doha-Qatar

***Abstract*— Privacy concerns are paramount in the adoption of new technologies, influencing user trust and regulatory landscapes. Connected vehicles produce vast amounts of real-time data, including driving behavior, location, and personal preferences, driven by the rapidly developing 5G technology and collaboration between the tech and automotive companies, making privacy an even more critical concern. The digitally connected network of vehicles and devices complicates the privacy problem further, necessitating updates to existing connected vehicle-related privacy frameworks to comply with current requirements. This paper explores the relevancy of the IEEE Digital Privacy Model (DPM) in the context of connected vehicles (C-V2X). The paper attempts to analyze in-depth how DPM promotes and encourages standardization and interoperability among stakeholders to address privacy challenges and enhance customer trust in connected vehicle technology. It also highlights the significance of Privacy by Design (PbD) concepts for proactive privacy protection and transparency in data practices. The IEEE DPM is outlined as a key framework for protecting privacy in the ecosystem of connected vehicles, guaranteeing adherence to various regulatory requirements, fostering secure data management practices, and encouraging the development of privacy-enhancing technologies for tackling future challenges.**

Connected vehicles, automobiles equipped for wireless communication, form a network exchanging data (location, speed, sensor readings) via vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) protocols. The potential of connected vehicles to enhance road safety through wireless communication and prevent accidents by exchanging data between vehicles and infrastructure is immense. Notably, this technology offers unexpected advantages in portability and cost compared to existing high-end vehicle technologies like radar and cameras, which are typically more expensive, less versatile and less portable. Connected vehicles can provide early alerts and significantly reduce accidents more efficiently. The concept of connected vehicles has a robust historical foundation, beginning with the Intermodal Surface Transportation Efficiency Act (ISTEA) of 1991, which initiated research into intelligent transportation systems (ITS) and vehicle-to-infrastructure communication. Key milestones in developing connected vehicle technology include GM's OnStar system and the establishment of IEEE Standard 802.11p and LTE Release 15, significantly accelerating its adoption [1, 2]. Despite the well-documented safety benefits and advancements, the mandatory deployment of connected vehicle technology remains limited. This is due to unresolved challenges like privacy concerns and data security issues [3]. This gap highlights the need for further research and policy development to address these barriers and fully leverage the potential of connected vehicles for road safety [4, 5].

Connected vehicles have significant advantages over new technologies now appearing in high-end vehicles, such as radar, LIDAR, cameras, and other sensors. For one thing, connected vehicle technologies and applications have a greater range than on-board vehicle equipment, allowing you to receive alerts of hazardous situations much earlier, providing more time to react and prevent an accident. Also, unlike radar, connected vehicle technology doesn't depend on “line of sight” communications to be effective. So, if a car ahead of you is braking hard on the other side of a hill due to an obstruction, you would receive notification even though you can't see and aren't aware of the dangerous situation developing. Connected vehicle technology is also less expensive to install than radar and camera equipment in vehicles. This will enable it to become standard equipment in the future on practically all vehicles, not just luxury cars.

Despite near universal agreement that mandatory deployment of connected vehicle technology could significantly improve road safety, reduce traffic congestion and streamline commercial vehicle operations, North American lawmakers have not yet been persuaded that the benefits outweigh the deployment challenges. Proponents have focused on using basic safety data from connected vehicles to reduce road accidents and save lives by identifying and drawing a driver’s immediate attention to hazardous situations. However, they have not discussed using connected vehicle data to conduct road safety analysis and road management, considerably enhancing the value proposition and making the case for mandatory deployment even more compelling. Moreover, the rapid pace of technological innovation continues to outstrip the development of privacy protections, leading to ongoing challenges. Issues such as data breaches, surveillance, and the ethical use of artificial intelligence highlight the need for continuous evolution in privacy practices and legal protections [6]. This underscores the importance of ongoing research and policy development to safeguard digital privacy in an increasingly connected world [7].

The philosophical underpinnings of privacy have been debated since the Enlightenment, but it is in the digital era that privacy concerns have become more pronounced and multifaceted. As technology advances, so do the harm to personal privacy, necessitating robust and adaptive responses. Legal frameworks such as the General Data Protection Regulation (GDPR) have been instrumental in setting data protection and privacy rights standards in the digital landscape [8]. Similarly, the concept of Privacy by Design, introduced by Ann Cavoukian, represents a paradigm shift in how privacy is integrated into technology development processes, ensuring that privacy considerations are fundamental to system architecture rather than an afterthought [9].

Privacy in connected vehicles presents unique challenges compared to other domains, such as medical or financial scenarios. In connected vehicles, privacy operates at the edge, dealing directly with data generated by the vehicle, while in financial contexts, privacy is managed at the core, dealing with centralized, sensitive information. Medical data primarily aligns with a core model, but it can also involve edge elements depending on the specific Use cases. The use cases in connected vehicles are more complex and varied than those in other areas. Recent reports have highlighted extensive privacy violations by major car manufacturers, raising significant concerns about unauthorized data collection, lack of transparency, and limited user control [10, 11]. These violations underscore the pressing need for robust privacy protections. The primary challenges include managing the vast amounts of data generated by connected vehicles, ensuring end-to-end privacy throughout data transmission, and balancing privacy with other important interests such as safety and convenience.

Digital privacy for connected vehicles began to attract significant attention in 2015, but nearly a decade later, few concerns have been addressed or resolved; efforts are hampered by overloaded terminology and lack of clarity concerning use cases [12]. Addressing these privacy issues requires a multifaceted approach involving clear user consent mechanisms, transparent data practices, and enhanced user control over personal information. By tackling these challenges, the potential of connected vehicles to improve road safety and enhance user experiences can be fully realized without compromising privacy.

The major contribution of this paper is the following:

1. Comprehensive review of the History of Connected Vehicles and the Evolution of Privacy Concerns in Connected Vehicles. This article introduces the three major categories of Connected Vehicles for the first time.
2. Proposing the IEEE DPM and its utility to Connected Vehicles, which is different from the other digital contemporizes
3. Discussing the opportunity of utilizing IEEE DPM for various use cases of Connected Vehicles
4. The rest of the paper is divided into providing a brief history of Connected Vehicles and Privacy Concerns, specifically highlighting the burning concerns in the past 10 years, and introducing the different categories of Connected Vehicles.

## BRIEF HISTORY OF CONNECTED VEHICLES AND PRIVACY CONCERNS

The ISTEA, the Intermodal Surface Transportation Efficiency Act, enacted in 1991 in the United States, was a pivotal legislation that catalyzed technology integration into transportation systems. It allocated funding for research and development initiatives to enhance transportation efficiency and safety. This support facilitated the early exploration of emerging technologies, including intelligent transportation systems (ITS) and vehicle-to-infrastructure (V2I) communication, focusing on improving efficiency, safety, and environmental sustainability. While ITS initially concentrated on traffic management and toll collection, it paved the way for later endeavors to integrate connectivity into vehicles and infrastructure. Moreover, ISTEA underscored the significance of data collection and sharing for transportation planning and management, establishing the groundwork for modern connected vehicle initiatives that leverage real-time data exchange to enhance safety and mobility.

Crucial milestones in connected vehicle (CV) technology encompass GM's OnStar introduction in 1995, the 2010 release of IEEE Standard 802.11p for Dedicated Short-Range Communications (DSRC), and the 2017 ratification of LTE Release 15, ushering in Cellular V2X (C-V2X). However, the widespread adoption was propelled by the emergence of 5G, driven by its cost-effectiveness. Several Tier One automobile manufacturers collaborate with entities such as Google, Microsoft, and Ericsson to harness connected vehicle technology to enhance the customer experience and fulfil commercial objectives.

Privacy is an intricate and diverse notion that has changed substantially in the digital era. Privacy is the right of individuals to control the collection, use, and dissemination of their personal information. In our increasingly digital environment, where the collection and utilization of personal data have become more prevalent, privacy is a fundamental concern. It is impossible to exaggerate how essential privacy is in the current era. Privacy violations are becoming increasingly common in a world where data breaches, surveillance, and data mining are the norm. These violations can result in harms to the individuals such as identity theft, discrimination, and loss of personal autonomy. Strong privacy protections and a thorough awareness of privacy's ethical, legal, and social aspects are more important than ever as society works through the challenges of the digital age.

Privacy concerns have emerged as significant barriers to the advancement of connected vehicles, as these vehicles generate and transmit vast amounts of personal data, including location information, driving behavior, and vehicle diagnostics. The collection and sharing of such sensitive data raise profound privacy concerns, encompassing issues such as constant surveillance, data security risks, and potential infringements on individuals' autonomy. Furthermore, the interconnected nature of connected vehicle systems increases the risk of data breaches and unauthorized access, while data-sharing practices among manufacturers, service providers, and other stakeholders raise questions about consent, control, and potential profiling. Adhering to privacy regulations such as GDPR and CCPA adds further complexity, necessitating robust privacy by design principles, transparency in data practices, and user-friendly privacy controls to address these concerns and foster trust among consumers, regulators, and industry stakeholders.

Privacy concerns in connected vehicles, characterized by the continuous generation and transmission of vast amounts of real-time data, present unique challenges that demand sophisticated privacy solutions to address privacy risks' dynamic and complex nature [13, 14]. The extensive data collection, encompassing location information, driving patterns, and biometric data, raises concerns about real-time tracking and surveillance, necessitating robust privacy measures that safeguard user privacy without compromising system functionality [15]. The interconnectedness of vehicle-to-everything (V2X) communication exacerbates the potential consequences of privacy breaches, impacting both individual drivers and the broader transportation ecosystem. Moreover, integrating multiple data sources in connected vehicles amplifies the risk of inferred data breaches, where seemingly anonymized data can be re-identified through advanced analytics, posing significant privacy challenges specific to the connected vehicle. To address these challenges, privacy-enhancing technologies (PETs) are crucial for preserving privacy, ensuring secure data transmission, and protecting user information from unauthorized access. Solutions such as blockchain-enabled security algorithms and differential privacy mechanisms offer effective strategies for maintaining privacy in connected vehicle environments, safeguarding sensitive data, and fostering user trust.

The advent of databases has significantly altered the privacy landscape, raising concerns about data security, unauthorized access, and potential misuse. With the centralization of vast amounts of personal information, individuals can be harmed by increased risks of identity theft, data breaches, and surveillance. Moreover, the linkage of disparate data sets within databases enables the creation of comprehensive profiles of individuals, eroding anonymity and posing harms to privacy. In response to these challenges, the concept of privacy by design has emerged as a proactive approach to address privacy concerns at every stage of the design and development process.

The concept of "Privacy by Design" is fundamental to privacy concerns in the digital age [9]. It was proposed by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, in the 1990s. Privacy by Design (PbD) is a framework aiming to embed privacy and data protection measures into the design and operation of systems, processes, and technologies from the outset. The core principles, refer to Figure 1, of PbD advocate

for proactive privacy measures, making privacy the default setting, integrating privacy features into design architecture, ensuring full functionality without compromising privacy, implementing end-to-end security, providing visibility and transparency to users about data practices, and respecting user privacy preferences. PbD emphasizes anticipating and preventing privacy-invasive events rather than reacting after the fact, and it promotes clear communication and user control over personal data. Widely recognized as a best practice, PbD has been incorporated into various privacy laws and regulations globally, empowering organizations to enhance trust, mitigate risks, and uphold privacy rights in an increasingly data-driven society.

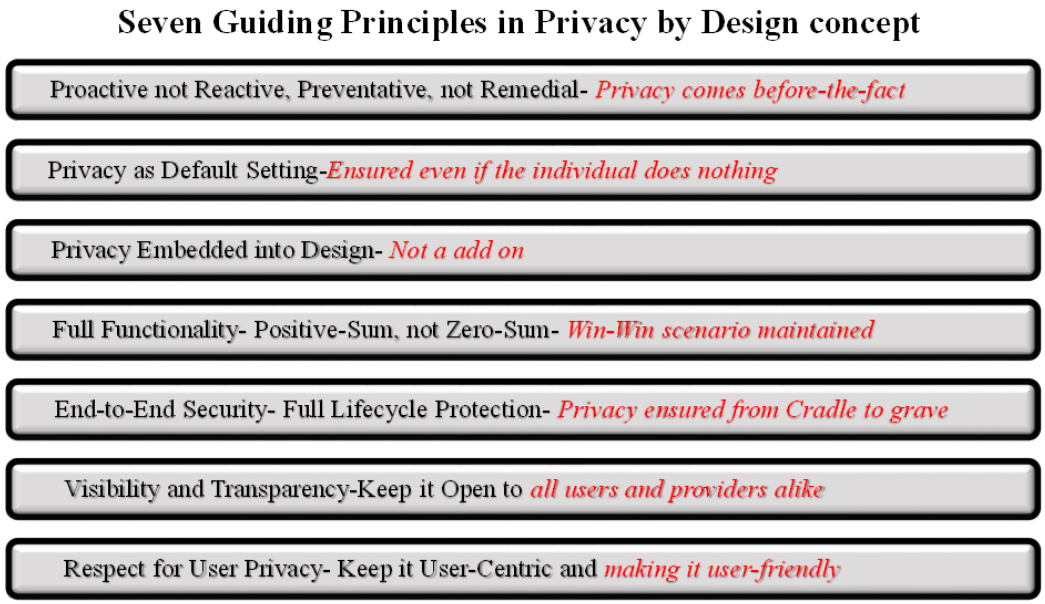


**Figure 1**. Seven Guiding Principles in Privacy by Design Concept

Cyber-physical systems (CPS) represent the integration of computational and physical components to monitor, control, and interact with the physical world. In the context of connected vehicles, CPS plays a pivotal role in transforming traditional automobiles into smart, interconnected entities capable of exchanging data with other vehicles, infrastructure, and external systems. Through embedded sensors, actuators, and communication technologies, connected vehicles can gather real-time data about their surroundings, including traffic conditions, road hazards, and weather patterns. This data is processed and analyzed by onboard computers to optimize vehicle operations, enhance safety, and improve the overall driving experience.

However, integrating CPS in connected vehicles also raises significant privacy concerns. With the collection and sharing of vast amounts of personal and vehicle-related data, individuals' privacy becomes increasingly vulnerable to exploitation and misuse. For example, location data, driving patterns, and vehicle diagnostics collected by connected vehicles can track individuals' movements, infer sensitive information about their daily routines, and even expose them to risks such as stalking or identity theft. Moreover, sharing this data with third parties, such as automotive manufacturers, service providers, and government agencies, raises questions about data ownership, consent, and control.

In such a system, privacy concerns are more prominent due to the inherent interconnectedness of CPS, which amplifies the potential for data collection, aggregation, and sharing. As connected vehicles become more

prevalent on our roads, addressing these privacy concerns becomes paramount to protecting individuals' rights while realizing CPS's transformative benefits in transportation.

Privacy by Design (PbD) faces several challenges in the context of connected vehicle systems, leading to potential shortcomings in privacy protection. The complexity of managing vast amounts of diverse data generated by connected vehicles, including location information, driving behavior, and vehicle diagnostics, presents a significant hurdle to implementing PbD principles effectively. Furthermore, the interconnected nature of the connected vehicle ecosystem, involving various stakeholders such as manufacturers, service providers, and government agencies, introduces complexities in ensuring end-to-end privacy protection. Third-party involvement, user expectations and behaviors, and regulatory compliance further complicate efforts to embed privacy protections into the design and operation of connected vehicle systems. Balancing the desire for innovative features and services with the need to uphold individuals' privacy rights requires a nuanced approach that addresses technical, legal, ethical, and societal considerations, highlighting the ongoing challenges in achieving privacy by design in this rapidly evolving domain.

In addition to the technical complexities, privacy by design in connected vehicle systems can fail due to the inherent tension between privacy and other competing interests, such as safety, convenience, and business interests. Manufacturers and service providers may prioritize functionality and user experience over stringent privacy protections, leading to compromises in privacy by design implementations. Moreover, the lack of standardized privacy protocols and practices across the automotive industry can result in inconsistencies and gaps in privacy protection measures. The evolving nature of technology and the emergence of new data-driven services and applications further exacerbate these challenges, requiring continuous adaptation and refinement of privacy by design strategies to keep pace with developments in the connected vehicle ecosystem. As connected vehicles become increasingly integrated into our daily lives, addressing these challenges is essential to ensure that privacy remains a fundamental consideration in designing and deploying connected vehicle systems.

Over the last 10 years, a steady stream of reports and publications that digital privacy is connected vehicular system cannot be taken for granted and perhaps the worst of any category that some authors have studied. A recent BC FIPA report [16] report iterates that CV’s gather extensive data, including driving behavior, location, biometrics, personal communications, web browsing history, and even music preferences. The collected data can be used for various purposes beyond improving vehicle systems, such as for targeted marketing, insurance pricing (UBI), and potentially by governments or malicious actors. Existing data protection laws seem inadequate to address these concerns, and industry self-regulation efforts fall short. Another Report by the Mozilla Foundation [17] exposes extensive privacy violations by major car manufacturers. The report reveals that nearly all car brands examined (25 including BMW, Ford, Toyota, Tesla) collect a vast amount of personal data, ranging from sensitive information like sexual activity and health data to facial expressions. This data collection occurs through in-vehicle sensors, microphones, cameras, and even phones and apps connected to the car. Privacy violations extend beyond data collection. The report identifies several concerning practices:

- Data Sharing: Manufacturers can share or sell this personal data to third parties such as [18], including data brokers and law enforcement, with broad justifications like "good faith" need.
- Lack of Transparency: Privacy policies are often lengthy, confusing, and difficult to understand, making it hard for consumers to know what data is collected and how it's used.
- Limited User Control: Consumers have minimal options to opt-out or control data collection. Sometimes, not using connected features may render the car's functionality inoperable.

Specific examples highlight the severity:

- Nissan: Explicitly admits to collecting data on sexual activity, health diagnosis, and even genetic information in their privacy policy, but without specifying how it's used.
- Kia: Collects information about your "sex life" according to their privacy policy.
- Mercedes-Benz: Manufactures certain models with TikTok pre-installed, raising concerns about data collection practices of a separate app.

These practices are concerning because they represent a large-scale collection of highly personal data without clear user consent or control. This data can be used for targeted advertising but also raises possibilities of discrimination, stalking, or even manipulation. The lack of transparency and user control exacerbates these risks.

Recently, Ghane et al. [11] discussed the privacy challenge in Intelligent Transportation Systems (ITS), where data collection relies on potentially untrusted edge controllers. They also mentioned how existing differential privacy methods struggle in such scenarios, particularly when dealing with correlated data like location and speed. Some recent applications, such as CarPlay and Android Auto, offer convenient integration of smartphone features within a vehicle's infotainment system [19]. However, their use raises privacy concerns that must be addressed in connected vehicle projects.

- Data Collection and Sharing: CarPlay and Android Auto collect user data, including location information, trip details, phone contacts, and potentially voice commands. The extent of data sharing with car manufacturers and app developers is a concern, particularly with Android Auto. This data could be used for targeted advertising, in-car recommendations, or shared with third parties. Connected vehicle projects raise additional concerns about potential access to car data (engine performance, diagnostics) by CarPlay/Android Auto. This data could be used for driver profiling, targeted marketing, or insurance adjustments.
- Security Risks: Integration of CarPlay/Android Auto introduces potential security vulnerabilities that hackers could exploit to gain access to car systems or steal data [20].
- Impact on Connected Vehicle Projects:
    - User Trust: Privacy concerns can lead to users' hesitation in adopting connected car features. Transparency around data collection and usage is vital for building trust.
    - Data Ownership: A clear understanding of data ownership (CarPlay/Android Auto, car systems) is essential. Connected vehicle projects need data ownership policies that protect user privacy [21].
    - Regulatory Landscape: Compliance with evolving data privacy regulations is crucial for responsible data handling in connected vehicle projects [21].

**DIFFERENT CATEGORIES OF CONNECTED VEHICLES**

The authors also would like to bring to the notice that the connected vehicle term is overloaded and can be categorized into three main categories, refer to Figure 2:

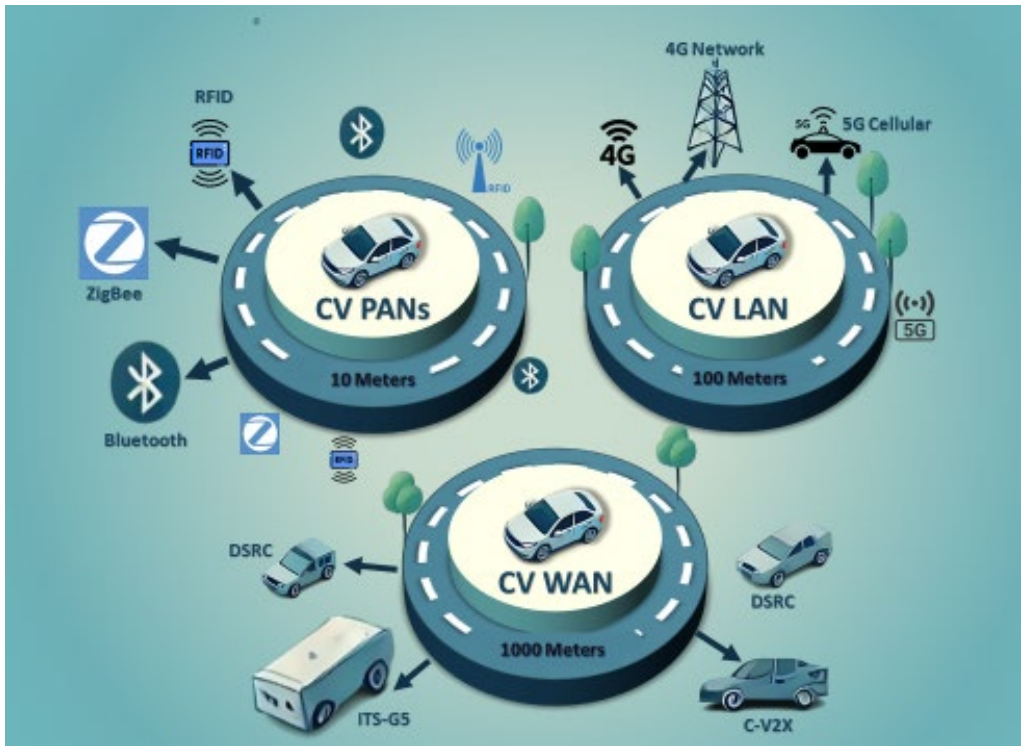


**Figure 2.** Different Categories of Connected Vehicles

- CV Personal Area Networks (CV PANs), often called Vehicle Area Networks, function at limited ranges of a few meters. They provide short-range connections using technologies like Bluetooth, ZigBee, or RFID to enhance driving convenience [22]. Ensuring secure and reliable interactions inside these networks is contingent upon resolving the cyber vulnerabilities present in CV PANs.
- CV Local Area Networks (CV LANs), also called Road Area Networks, are networks extending over hundreds of meters. To provide connectivity for crucial applications like traffic management and collision avoidance, they typically employ technologies like ITS-G5, C-V2X, and DSRC. These networks facilitate local communication and data exchange, which is crucial for improving road safety and optimizing traffic flow [23].
- Wide Area Networks (CV WANs), also called Cellular Networks, are networks that span thousands of meters and are powered by 4G or 5G cellular technologies. CV WANs are essential for sharing traffic data over large distances, facilitating connections with susceptible road users, and uploading vehicle data to private clouds. Their wide coverage and high data transfer rates make them indispensable for connectivity and large-scale data management in linked car systems [24].

These CV technologies have distinct capabilities, support distinct use cases, and should not be conflated.

**PRIVACY CONCERNS IN CV DIFFERENT FROM OTHER DOMAINS**

Privacy considerations in Connected Vehicle use cases diverge from those in Medical or Financial scenarios, where the privacy concerns are not as concerning and have been taken care of to a larger extent [25]. The medical or financial scenarios approaches cannot be replicated in Connected Vehicles. To grasp this disparity, it's essential to comprehend Privacy at the Edge (representing Connected Vehicles' privacy) and Privacy at the Core (symbolizing privacy in Medical or Financial contexts). "Privacy at the edge" and

"privacy at the core" refer to different approaches to managing and protecting data privacy in computing systems, particularly in the context of distributed computing architectures such as edge computing and cloud computing [26].

o Privacy at the Edge:
In edge computing, data processing and storage are decentralized and distributed closer to the data source, such as IoT devices, sensors, or edge servers at the network edge. Privacy at the edge focuses on implementing privacy protections and controls directly at the edge devices or edge computing nodes where data is generated and processed. This approach aims to minimize data transmission to centralized cloud servers, reducing the risk of data exposure, unauthorized access, or interception during transit. Privacy at the edge may involve data anonymization, encryption, access controls, and local processing of sensitive data to ensure privacy and compliance with privacy regulations [27].

o Privacy at the Core:
In cloud computing, data processing and storage are centralized in remote data centers (the "core" or "cloud") and are managed by cloud service providers. Privacy at the core focuses on implementing privacy protections and controls within the centralized cloud infrastructure, such as encryption, access controls, data masking, and audit trails. This approach assumes that data transmitted to and stored in the cloud is secure and protected against unauthorized access or breaches. Privacy at the core may involve leveraging cloud service providers' security features and compliance certifications to ensure data privacy and regulatory compliance [28].
While both approaches aim to protect data privacy, they differ in their emphasis on where and how privacy controls are implemented. Here's how connected vehicles differ from medical and financial use cases:

o Medical Data:
In healthcare, patient data is highly sensitive and subject to strict regulations like HIPAA (Health Insurance Portability and Accountability Act) in the US [29]. This often necessitates a privacy-at-core approach. Patient data is typically stored securely in centralized medical databases with robust access controls and encryption to minimize the risk of unauthorized access or breaches. While some edge processing might occur (e.g., on wearable health monitors), the focus remains on safeguarding sensitive medical information within a controlled environment [30].

o Financial Data: Financial data, such as account information and transaction detail, also requires strong privacy protections. Here, a hybrid approach might be used. Some institutions might leverage privacy-at-core by storing sensitive financial data in secure, centralized databases [31]. However, edge computing can also play a role. For example, fingerprint or facial recognition for mobile banking applications might involve some processing at the edge device to enhance security while minimizing the amount of sensitive biometric data transmitted.

o Connected Vehicle Data: Connected vehicles collect a range of data, including location, speed, and sensor readings. While not as inherently sensitive as medical data, this information can still reveal a lot about a driver's habits, routines, and potentially even health conditions [32]. Here, the balance between privacy and functionality becomes crucial. Privacy-at-the-edge can be beneficial by anonymizing or aggregating data before transmission, reducing the risk of re-identification and unauthorized access. Additionally, leveraging federated learning at the edge allows collaborative learning on anonymized data for traffic optimization or anomaly detection without compromising individual privacy. However, some functionalities might still necessitate centralized data storage and processing (e.g., real-time traffic updates). Finding the optimal balance between privacy-enhancing techniques at the edge and secure data aggregation at the core is key for connected vehicles.

## IEEE DIGITAL PRIVACY MODEL

The rising concerns about privacy have resulted in the creation of the IEEE Digital Privacy Initiative (DPI). The IEEE Digital Privacy Initiative (DPI) was established to address the growing importance of privacy in the digital age and to promote the development of standards and best practices for protecting individuals' privacy rights. IEEE DPI developed the Digital Privacy Model (DPM) as shown in Figure 3.

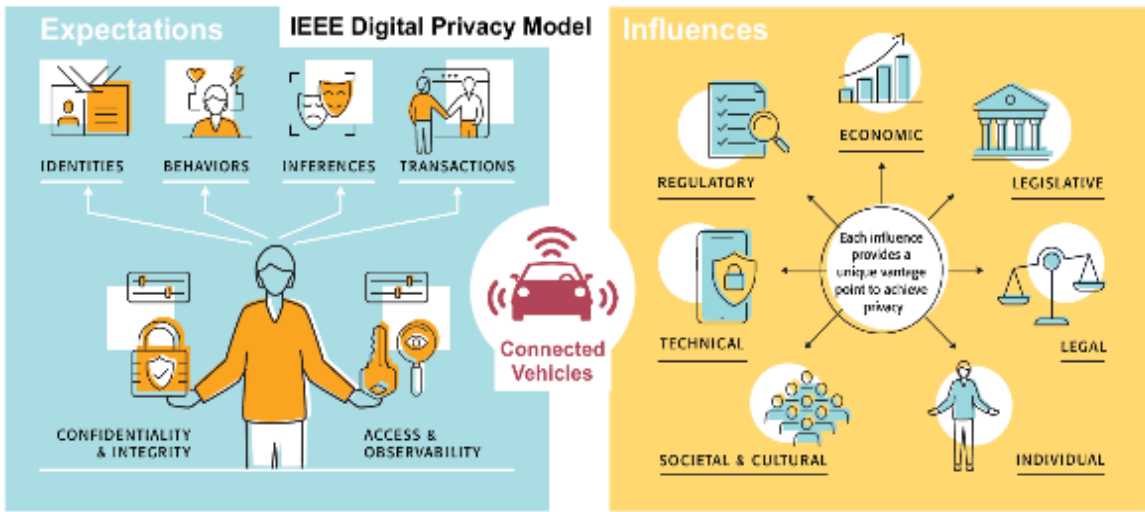


**Figure 3.** IEEE Digital Privacy Model

The IEEE DPM aims to balance the benefits of data sharing in connected vehicles and driver privacy concerns. It emphasizes informed consent, requiring users to understand the data collected, its purpose, and potential risks before agreeing to share it. The IEEE DPM also recognizes that there are environmental influences such as societal and economic ones on digital privacy.

The model addresses various data categories:

- Identities (PII): The model considers how to protect personally identifiable information like name, license number, medical conditions, and insurance details.
- Behaviors: Techniques to prevent revealing driving habits and patterns (e.g., frequent destinations) might be part of the model.
- Inferences: The model addresses how to limit the ability to infer sensitive information from data (e.g., health conditions from driving patterns).
- Transactions: The model ensures secure data exchange between connected vehicles and other entities, protecting data integrity during transactions.

In the rapidly changing digital landscape, user privacy and personal data protection are critical, and the IEEE Digital Privacy Model (DPM) has become an indispensable framework. The DPM emerged in response to the inadequacies of traditional privacy approaches caused by the complexities introduced by cutting-edge technologies like big data, IoT, and AI. This model offers a comprehensive and flexible approach to privacy, tailored to meet the challenges presented by contemporary digital environments. It integrates diverse insights from technologists, legal experts, policymakers, and industry leaders. Its fundamental tenets—Privacy by Design, User-Centric Privacy, Data Minimization, Transparency and Accountability, Security Measures, and Regulation Compliance—guarantee that privacy is an integral part of digital systems and not an afterthought.

The DPM's scope is broad, encompassing a range of technological contexts and industries. It can be used in many industries, including healthcare, banking, retail, and education, all with different privacy requirements. For example, the DPM protects patient information on telemedicine platforms and electronic health records in the healthcare industry. In the financial industry, it protects client privacy during banking and transactional activities. The model holds equal significance for blockchain, cloud computing, AI, and IoT technologies. The DPM's relevance and applicability are increased because it offers a flexible framework that enables organizations to tailor their privacy policies to their unique operational and technological contexts.

The DPM's involvement in regulatory compliance is one of its major contributions. Organizations must comply with increasingly strict privacy regulations, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA), to avoid legal ramifications. The DPM offers structured guidelines incorporating privacy practices into compliance strategies, helping businesses navigate this complex regulatory landscape. This methodical approach streamlines compliance with international privacy standards, assisting businesses in avoiding penalties and legal issues while guaranteeing strong personal data protection.

The DPM strongly emphasizes building consumer trust and promoting innovation in addition to compliance. The model contributes to establishing and preserving consumer and organizational trust by promoting transparency and user control. Furthermore, it encourages the creation of privacy-preserving methods and tools, such as ethical AI and privacy-enhancing technologies (PETs). The DPM fosters an atmosphere where innovation can flourish without jeopardizing user confidence or data security by balancing the need for privacy protection and the desire for technological advancement.

## IEEE DPM UTILITY IN CONNECTED VEHICLES AND ITS USE CASES

The need to handle particular privacy issues posed by these technologies is why DPM is crucial in connected cars. Large amounts of data are produced by connected cars, including location, driving habits, and personal preferences. If these data are not adequately safeguarded, they may be misused. DPM offers a framework for handling data responsibly, guaranteeing adherence to privacy regulations, and building user trust. Connected car systems can steer clear of legal problems and boost user confidence in the technology by putting privacy first.

Connected Vehicles (CV) represent a significant advancement in automotive technology, incorporating internet connectivity and various data-driven services to enhance the driving experience. Implementing the DPM in CVs is to protect user data and improve privacy. Data minimization is crucial in the first place because it lowers exposure risk by only gathering data that is required for particular functions. Techniques like anonymization and pseudonymization further protect user identities by making data interception less revealing. Building trust and adhering to privacy regulations is ensured by obtaining explicit user consent for data collection and processing, along with clear usage explanations. Strong security measures are essential for preventing unauthorized access to data and data breaches. These measures include encryption and secure communication protocols.

Ultimately, DPM implementation fosters innovation in the automotive sector while guaranteeing safe and private operations. Manufacturers and service providers can encourage the development of cutting-edge, privacy-preserving technologies by upholding privacy standards. The DPM framework protects user data while advancing technology by assisting connected cars in operating within changing privacy standards.

The IEEE Digital Privacy Model (DPM) provides a comprehensive framework to address privacy concerns in various use cases of connected vehicles, refer to Figure 4, ensuring privacy protection and regulatory compliance.

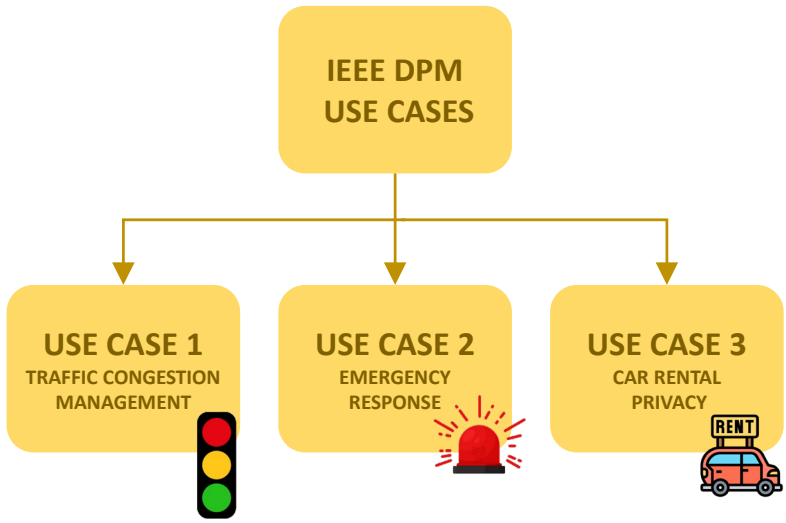


**Figure 4.** IEEE DPM USE CASES

• Use Case 1: Traffic Congestion Management
Traffic congestion management presents a strong use case for implementing IEEE DPM in connected vehicles (CV). This scenario imagines a city where connected cars interact with road infrastructure and traffic lights to maximize traffic flow. To efficiently manage traffic, real-time location data and speed information are shared. Vehicle counts, occupancy, density, and origin-destination data should all be included in the collected data to preserve privacy, but individual identities must remain anonymous. Speed and location data should be kept private to prevent origin-destination information from being readily corroborated with personal identifiers. The data allows for inferring general traffic patterns without disclosing specific driving behaviors. Secure communication protocols are necessary to safeguard the data's confidentiality and integrity and stop illegal access and manipulation. Implementing secure communication protocols and efficient anonymization techniques are technical considerations, and regulatory frameworks may require data anonymization and limit access to personal data. Legislative action may be needed to address data ownership and liability issues, and economically viable infrastructure updates and data collection solutions are imperative. While people should be responsible for how their anonymized data is used, legal frameworks should guarantee data security and guard against abuse. Societal and cultural factors emphasize the importance of public trust in data security to encourage the widespread adoption of such technologies.

• Use Case 2: Emergency Response
Emergency response is a crucial use case in the field of IEEE DPM, which is applied to connected vehicles (CVs) and emphasizes the need to handle sensitive data. In this case, if a connected car gets into an accident, it can automatically send location information, use severity sensors to initiate an emergency call, and have integrated medical devices to track the car's vital signs. There are strict expectations regarding data privacy in this situation: personal information should only be disclosed to authorized emergency personnel, medical records must be kept private, and accident details must be accurate. Behaviors are not important in this case, but the transmitted data can provide information about the location and severity of the accident. Strong data encryption and secure communication protocols are necessary to safeguard the integrity and confidentiality of

accident and medical data. Relevant information must be accessible to emergency responders, but unauthorized access must be severely limited. Regulations may specify who can access this data and the extent of data transmission acceptable in emergencies. The expenses of installing these emergency response systems in cars are one area of economic concern. Legislative frameworks should guarantee data security and responders' appropriate use, and legislative measures might address privacy exceptions in emergency situations. Furthermore, even in dire circumstances, people should be in charge of how their medical data is used.

• Use Case 3: Car Rental Privacy
Car rental privacy poses a major challenge in the context of IEEE DPM for connected vehicles. When a customer rents a car, the infotainment system and telematics unit gather data, including credit card details, name, and driver's license information. This data must be safely stored and used only for rental purposes. To streamline fleet management and simplify billing, the vehicle also collects information on location, mileage, rental time, and fuel consumption without monitoring individual driver habits. The vehicle, the rental company's systems, and payment processors must securely exchange information regarding rental agreements, start and end locations, and payments. The rental company has access to the data required for fleet management, billing, and customer service, while customer access is restricted to rental agreement details and anonymized trip summaries. Technical factors include methods for anonymizing data, safe data storage, and explicit opt-in/opt-out choices for further data collection. User control over data access, security standards, and data minimization may be mandated by regulatory requirements. In addition to addressing data ownership, potential liability, and ensuring data security, legislative and legal frameworks should strike an economic balance between the benefits of data and privacy measures. Lastly, customers should be provided with clear information about data practices and opt-out options to encourage public awareness and informed consent regarding data privacy in car rentals.

The concept of privacy is becoming more complicated in the digital age due to the widespread collection of personal data and the quick development of technology. This study looked at how privacy is changing, especially with regard to connected cars, and how the IEEE Digital Privacy Model (DPM) attempts to address these issues.

The IEEE Digital Privacy Model (DPM) is particularly crucial for connected vehicles due to the unique nature of the data they generate. Unlike static data from industries like healthcare or banking, connected vehicles produce real-time position, speed, and route data, which require ongoing tracking of people's movements. The DPM anonymizes and encrypts this vast amount of dynamic data to prevent misuse, address safety concerns, and protect user privacy. The automotive industry faces complex international privacy regulations, unlike the more uniform frameworks in healthcare or banking. The DPM's standardized approach helps navigate these diverse laws, ensuring compliance across jurisdictions. This is vital for building consumer trust in connected vehicles, which is less of an issue in more established sectors.

The connected car ecosystem also involves various stakeholders, including infrastructure operators, technology providers, and manufacturers. The DPM promotes standardization and interoperability, ensuring consistent privacy policies across these diverse organizations. Advanced technologies like IoT, AI, and real-time data processing are integral to connected vehicles. The DPM provides safe data management and privacy principles in this evolving field.
In summary, incorporating privacy frameworks such as the IEEE DPM into emerging technologies is crucial for safeguarding individual rights and promoting public trust as we navigate the intricacies of the digital era. By incorporating advanced privacy-enhancing techniques and prioritizing privacy from the design phase, we can guarantee that technological advancements advance society without jeopardizing core privacy principles.

The continued development and improvement of these strategies will be essential to solving privacy issues in the future and creating a safe, secure digital environment.

## REFERENCES


[1] S. Smith, J. Bellone, S. Bransfield, A. Ingles, G. Noel, E. Reed, et al., "Benefits estimation framework for automated vehicle operations," United States. Department of Transportation. Intelligent Transportation …2015.

[2] W. Xiong and R. Lagerström, "Threat modeling–A systematic literature review," Computers & security, vol. 84 pp. 53-69(2019)

[3] S. Uysal and M. T. Sandıkkaya, "A survey on obstacles to the widespread use of connected and automated vehicles," Journal of Ambient Intelligence and Smart Environments, (Preprint), pp. 1-17(2024)

[4] S. Doecke, A. Grant, and R. W. Anderson, "The real-world safety potential of connected vehicle technology," Traffic injury prevention, vol. 16 (sup1), pp. S31-S35(2015)

[5] X. Li, Y. Yu, G. Sun, and K. Chen, "Connected vehicles' security from the perspective of the in-vehicle network," IEEE Network, vol. 32 (3), pp. 58-63(2018)

[6] L. Edwards and M. Veale, "Slave to the algorithm? Why a'right to an explanation'is probably not the remedy you are looking for," Duke L. & Tech. Rev., vol. 16 p. 18(2017)

[7] D. J. Solove, Understanding privacy: Harvard university press, 2010.

[8] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," Computer Law & Security Review, vol. 34 (1), pp. 134-153(2018)

A. Cavoukian, "Privacy by design: The 7 foundational principles," Information and privacy commissioner of Ontario, Canada, vol. 5 p. 12(2009)

[9] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions," IEEE Access, vol. 10 pp. 86127-86180(2022)

[10] S. Ghane, A. Jolfaei, L. Kulik, K. Ramamohanarao, and D. Puthal, "Preserving privacy in the internet of connected vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 22 (8), pp. 5018-5027(2020)

[11] T. Olovsson, T. Svensson, and J. Wu, "Future connected vehicles: Communications demands, privacy and cyber-security," vol. 2, ed: Elsevier, 2022, p. 100056.

[12] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE, vol. 25 (8), 2007)

[13] J. Walter and B. Abendroth, "On the role of informational privacy in connected vehicles: A privacy-aware acceptance modelling approach for connected vehicular services," Telematics and Informatics, vol. 49 2020)

[14] J. Petit, D. Broekhuis, M. Feiri, and F. Kargl, "Connected Vehicles: Surveillance Threat and Mitigation," in Black Hat Europe.

[15] "The Connected Car: Who is in the Driver's Seat? " A study on privacy and onboard vehicle telematics technology," British Columbia Freedom of Information and Privacy Association2015.

[16] "Privacy Nightmare on Wheels': Every Car Brand Reviewed By Mozilla — Including Ford, Volkswagen and Toyota — Flunks Privacy Test," 2023.

[17] wejo. Available: https://www.wejo.com/.

[18] B. Nelson and T. Olovsson, "Introducing Differential Privacy to the Automotive Domain: Opportunities and Challenges," 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, 2017, pp. 1-7, doi: 10.1109/VTCFall.2017.8288389.

[19] E. Chatzoglou, G. Kambourakis, and V. Kouliaridis, "A multi-tier security analysis of official car management apps for Android," Future Internet, vol. 13, no. 3, p. 58, 2021. Available: https://doi.org/10.3390/fi13030058

[20] A. M. Soley, J. E. Siegel, D. Suo, and S. E. Sarma, "Value in vehicles: economic assessment of automotive data," Digital Policy, Regulation and Governance, vol. 20, no. 5, pp. 413–427, Oct. 2018.
[21] R. Coppola and M. Morisio, "Connected Car: Technologies, issues, future trends," ACM Computing Surveys, vol. 49, no. 3, Art. no. 46, pp. 1-36, Oct. 2016. Available: https://doi.org/10.1145/2971482
[22] P. Roux, S. Sesia, V. Mannoni and E. Perraud, "System Level Analysis for ITS-G5 and LTE-V2X Performance Comparison," 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Monterey, CA, USA, 2019, pp. 1-9, doi: 10.1109/MASS.2019.00010.
[23] M. Ahmed et al., "Vehicular Communication Network Enabled CAV Data Offloading: A Review," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 8, pp. 7869-7897, Aug. 2023, doi: 10.1109/TITS.2023.3263643.
[24] T. Nawrath, D. Fischer and B. Markscheffel, "Privacy-sensitive data in connected cars," 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 2016, pp. 392-393, doi: 10.1109/ICITST.2016.7856736.
[25] S. Guynes, J. Parrish, and R. Vedder, "Edge computing societal privacy and security issues," SIGCAS Computers and Society, vol. 48, no. 3–4, pp. 11–12, Sep. 2019.Available:https://doi.org/10.1145/3383641.3383643
[26] F. -Y. Rao and E. Bertino, "Privacy Techniques for Edge Computing Systems," in Proceedings of the IEEE, vol. 107, no. 8, pp. 1632-1654, Aug. 2019, doi: 10.1109/JPROC.2019.2918749.
[27] [28] Y. Shi, "Data Security and Privacy Protection in Public Cloud," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 4812-4819, doi: 10.1109/BigData.2018.8622531.
[28] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," Security and Communication Networks, vol. 2018, Art. no. 5978636, Mar. 2018. Available: https://doi.org/10.1155/2018/5978636
[29] N. Almusallam, A. Alabdulatif, and F. Alarfaj, "[Retracted] Analysis of privacy-preserving edge computing and Internet of Things models in healthcare domain," Security and Communication Networks, vol. 2021, Art. no. 6834800, Dec. 2021. Available: https://doi.org/10.1155/2021/6834800
[30] World Economic Forum, The Next Generation of Data Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value, Prepared in collaboration with Deloitte, Geneva, Switzerland, Sep. 2019. Available: https://www.weforum.org
[31] N. Rizzo, E. Sprissler, Y. Hong and S. Goel, "Privacy preserving driving style recognition," 2015 International Conference on Connected Vehicles and Expo (ICCVE), Shenzhen, China, 2015, pp. 232-237, doi: 10.1109/ICCVE.2015.42.

**David G. Michelson** is a leading researcher in wireless propagation and intelligent transportation at the University of British Columbia, where he directs the Radio Science Lab and the AURORA Connected Vehicle Testbed. He chairs the IEEE Vancouver Chapter for Vehicular Technology and Intelligent Transportation Societies and holds key roles with ITS Canada and the Transportation Association of Canada. An active contributor to standards, Prof. Michelson chairs IEEE Standards Association Working Group P2982, the VT/MRSC Mobile Radio Standards Committee, and the URSI-ITU Inter-Union Working Group, among other positions. He was instrumental in enhancing IEEE VTS conferences, earning a VTS Conference Leadership Award for his contributions. Prof. Michelson also chairs the IEEE History Coordination Committee, fostering collaboration across IEEE's history initiatives. Contact him/her at davem@ece.ubc.ca.

**Amith Khandakar Md. Abdullah** is a distinguished researcher in Sensors and Instrumentation. He is currently teaching at the Electrical Engineering Department of Qatar University. As a prolific researcher, he has published over 100 journal papers, holds four registered U.S. patents. An IEEE Senior Member, and currently focusing on value proposition of the Connected Vehicle Technology. Contact him/her at amitk@qu.edu.qa.