"Baby, You Can Drive My Car" … and I Will Know Everything About You! Privacy and Data Protection Policies as Remedy to Digital Vulnerability

Alessandra Pera and Sara Rigazio

Abstract As the findings of the DiVE project have showed, we are all vulnerable in the digital domain. Starting from this assumption, the chapter delves into the notion of remedying vulnerability from a human-dignity centred perspective, focusing on data protection rules as one of the most appropriate legal instruments to deal with shortcomings of digital marketplaces. More in particular, the chapter takes inspiration from the 2024 Australian Toyota case. The car company was accused of illegitimately collecting and sharing its customers' data (race, facial expressions, weight, health and genetic information, location) with third parties, such as insurance companies, debt collector agencies, and data collection companies. The case is critical because it sparked a series of investigations into similar cases involving Toyota as well as other car manufacturers around the world, raising questions about the effectiveness of the remedies to protect users' privacy and data. The chapter argues that the legal answer to this should rely on a legal framework that encourages responsible innovation in the AI interactions, fostering the protection of fundamental rights, as recommended by the European Data Protection Board in its Opinion n. 28/2024. In this regard, the chapter embraces the 'Societal Structure Model' for privacy protection, and argues that privacy should be protected not only as an individual interest but also as an entitlement functional to the promotion of societal collective values such as democracy, freedom, transparency, and, most importantly, human dignity. The chapter unpacks

The title of the chapter is referring to the famous song by the Beatles 'Drive My Car'. It is a song primarily written by Paul McCartney, with lyrical contributions from John Lennon, and first released by the Beatles on the British version of the 1965 album Rubber Soul; it also appeared in North America on the Yesterday and Today collection. The upbeat, light-hearted 'Drive My Car' was used as the opening track for both albums. See https://www.thebeatles.com/drive-my-car. This chapter is the result of a common research and reflection of the two authors. For the purpose of research evaluations only, Alessandra Pera authored Sects. 2 and 3, while Sara Rigazio authored Sects. 4, 5 and 6. Sections 1 and 7 were co-authored.

A. Pera (✉) · S. Rigazio
Department of Political Science and International Relations, University of Palermo, Palermo, Italy
e-mail: alessandra.pera@unipa.it

S. Rigazio
e-mail: sara.rigazio@unipa.it

C. Crea and M. Infantino (eds.), *Remedies to Digital Vulnerability in European Private Law*, https://doi.org/10.1007/978-3-032-19720-7_20

how the different nuances of this model can help understand privacy as a common, public interest and shows the importance of institutions, policy makers, and stakeholders' collective response for promoting and empowering each of us in a healthy and productive interaction with technology.

Keywords Digital vulnerability · Connected cars · Data protection law · Privacy · Human dignity · Societal structure model

1 Introduction

Never has International Privacy Day—celebrated on January 28th each year—taken on such a vivid significance as it does this year: the repeated data breaches worldwide, the use of surveillance technologies, and the interventions by many national privacy authorities, have reminded us that, literally, we are living in a world immersed in the digital dimension and we have to pay a price to live in it. To illustrate with regard to data breaches, suffice it to mention what happened when the website of 23andMe, a US based American personal genomics and biotechnology company. The website was hacked in 2023, exposing genetic data of nearly 7 million people; in 2025, that same data was auctioned off in bankruptcy court.[1] Cases of illegitimate or at least ambiguous surveillance by private actors as well as governmental agencies now happen on a daily basis. On June 28, 2025, the Hungarian government installed and made use of hundreds of surveillance cameras in order to identify the participants to an unauthorised Pride manifestation; the surveillance cameras recorded biometric data of the participants in violation of the European Union (EU) Artificial Intelligence Act.[2] At the same time, independent agencies and privacy authorities have been busier than ever in their attempts to prevent violations of data protection laws. The Italian Data Protection Authority, for example, has led the way in the European child protection context with the Replika cases and, more recently, with the ChatGPT one.[3] Permeating every aspect of our life, technology, more often than not, simplifies many of our daily dynamics. From work up to the aspects of our personal and relational life, at any age,[4] technological tools prove to be not only ubiquitous but able to manage and dictate the times and ways of our habits and, therefore, our choices. Shoshana Zuboff

[1] The legal questions are many, but the common issue is clearly the role of data governance and of policymakers. On the specific topic of genetic information, see Sharma and Gordon (2025).

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

[3] See https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9906258.

[4] This is, for example, what we have previously investigated about smart toys and the use of the so-called AI girlfriend chatbots: see Pera and Rigazio (2024), Pera and Rigazio (2025).

coined the expression "surveillance capitalism" to refer to this systematic and one-sided reduction of the human experience into free-to-use, valuable information—that is, data.[5]

During these past three years, the DiVE project has demonstrated, under multiple perspectives, that we are all vulnerable in the digital dimension: although with different intensity, during different stages of our life—emotionally and biographically –, vulnerability is a constant of our existences.[6] Indeed, beneath the surface of convenience offered by technology, lies a quite troubling reality: most of the digital services are designed to extract and monetize our data with little or no regard for our privacy or autonomy. As it has been noted, this trade-off is a sort of "hidden tax" that, beyond our wallets, impacts the very fabric of our societies.[7]

As Stefano Rodotà reminds us, it is therefore imperative, for every democratic society, to prevent the person from becoming the object of powers that can falsify and construct his or her *persona* according to the needs of a society of surveillance, of social selection or of economic calculation.[8]

In this context, we will see that, even the most mundane, common action such as driving a car can represent a potential and a real threat. This is exactly what happens when a series of options called 'connected car services', such as, for example, geolocation or the ability to view videos from the car's surroundings, which depend on the transfer of data via the Internet, are activated and mismanaged. In this regard, the case of the data breach made by Toyota in Australia in 2024 represents a significant and useful case study, due to the popularity of the company among consumers worldwide and to the substantial share of the market held by the concerned company. The analysis of the modalities in which these services are offered by Toyota (as well as by many other car companies) will serve as a benchmark of the pervasiveness and the ambiguity of privacy policies and, at the same time, will inspire the search for solutions in this chapter.

In this regard, we strongly believe that privacy and data protection should remain at the core of any robust solution to protect and preserve the fundamental value of human dignity, for the benefit of society as a whole. In line with this idea, we argue that privacy following the 'societal structure model' would be a far more effective model than the current one based on privacy as purely an individual right. The 'social

[5] Zuboff (2019).

[6] The contributors of the DiVE project analysed the concept of vulnerability in the legal European framework under multiple facets, focussing in particular on groups of vulnerable people minors, elderly, consumers, and patients. Among the many who contributed to the vulnerability debate—besides Albertson Fineman (2009)—, see Mendola and Pera (2022), Malgieri and Niklas (2020), Calo (2017), Nussbaum (2000).

[7] The expression is by Monique Priestley, democratic representative in the Vermont House of Representatives, and an active supporter and proponent of a drastic privacy federal reform in the U.S. See https://vtdigger.org/2025/02/04/rep-monique-priestley-and-caitriona-fitzgerald-why-data-privacy-is-the-key-to-unlocking-affordability.

[8] Rodotà (2014). Rodotà was a pioneer in the study of the 'power of data' at the intersection between law and technology.

structure model' take on privacy, as Rodotà taught us,[9] aims at controlling the power of organizations when collecting and disclosing personal data, and at preventing harm to the entire society, creating a virtuous circle that makes possible a balanced co-existence between the real and digital self of each individual.

Our paper is organized as follows. After briefly outlining what connected car services consist of in Sect. 2, we analyse in Sect. 3 the issue at the heart of the 2024 Australian Toyota case, started in Australia, with particular reference to the type of data collected, used, and shared, and to its forms of management. We will provide useful food for thought in Sect. 4, taking inspiration from the European legal framework. We will look in particular from the European Data Protection Board (EDPB) Opinion No 28, published in December 2024,[10] which emphasized the need for responsible innovation and a human centric use of technology, and from the EDPB 2021 'Guidelines on processing personal data in the context of connected vehicles'.[11] These texts, together with other significant interventions by the EU, will help enlighten the issues at stake that, given the real-time circulation of data across national borders, are truly transnational issues. Section 5 will assess how the effectiveness of this legal framework to protection privacy. On this basis we will argue in Sect. 6 that the rise of AI, as the case of Toyota connected car services clearly shows, vividly calls for the necessity to re-think and to some extent re-invent the traditional paradigm of privacy—to be considered as public good and a public interest, in order to protect fundamental rights, especially when involving the minorities. Section 7 will conclude.

2 Connected Car Services

In order to properly introduce the topic, we need first to address briefly what the connected car services consist of, and how they work. According to a study on connected car services presented in 2015 to the European Commission, a connected car can be described "as a platform that enables the exchange of information between the car and its surroundings, either through local wireless networks or via the internet".[12] In other words, passenger vehicles that come equipped to transmit data about the car and its driver from the vehicle in real time via the Internet to the vehicle manufacturer and/or other businesses.

[9] Rodotà (2014). The author argues that each individual is made of these two entities, the latter being the collection of information that literally builds each person's character and personality such as the emotions, the feelings, the memories. The physical and the digital self are naturally connected, but the only way to ensure that the latter does not outweigh the first, is protecting and promoting the principle of dignity.

[10] EDPB (2024).

[11] EDPB (2021).

[12] See European Commission (2015, 5).

Typically, the possible interactions through this connectivity can be identified as: vehicle-to-vehicle (v2v) interactions, such as in the case of cars interacting with other cars; vehicle-to-infrastructure (v2i) or infrastructure-to-vehicle (i2v) interactions, when cars interact with (roadside) infrastructure and vice versa; vehicle-to-device (v2x) interactions, which consist of wireless communication to any device. Even if all these three types of interactions are meaningful in our debate, our considerations focus primarily on the last one.

Connected car services are certainly associated with some benefits. The first and most publicized is safety. Practically every car manufacturer and selling company advance the argument that improving safety is the ultimate goal of connected cars. How? By letting drivers stay fully informed of the current driving situation, thus allowing them to perform tasks such as planning the best route, forecasting traffic jams, and predicting the best time to schedule a trip.

Safety comes with other functions such as the geolocation, the possibility of using the car's camera to view the inside but also the surroundings of the car, the option of locking and unlocking the car automatically without a key by distance. Other features include SOS or emergency calls, remote checking of doors, anti-theft recorder and stolen vehicle tracking, avoidance of obstacles in the trajectory, and assistance with the driving direction through the support of video car's cameras.

On the one hand, when we look at the benefits, it is therefore clear that connected cars collect a goldmine of information that could be useful, for example, to improve any technical issues about the car, allowing data analysts to work on the problem and presumably solve it. On the other hand, we identify a series of potential risks and harms, the most immediate of which is, of course, privacy. Since the entire system works on the data entered, concerns arise on two levels: first of all, on the nature of the information gathered and, secondly, on the way the information is handled.

The first aspect is extremely relevant since information apparently classified as pertaining to the functioning of the vehicle (such as the number of times the brakes were used or the images recorded when parking for safety reasons) is in fact information that can identify people, and can therefore to be used for purposes completely unrelated to the technical functioning of the car. Interestingly, data lies at the core of connected cars' benefits as much as risks.

In relation to the way in which these services work, usually connected cars require the driver/owner to download the car's company app and then use the related connected services. Once the app is set up, data is generally transmitted to the car's manufacturer and/or other businesses or organizations. It is worth noticing that some pieces of information are transmitted directly without any previous consent by the driver/owner. In other cases, information may not be sent, but de-activating some functions may undermine the use of fundamental functions of the car.

3 The Toyota Case(S). My Car, My Data?

In September 2023 the Mozilla Foundation, a U.S. non-profit organization, published a study conducted on several popular car brands,[13] that compared their privacy policies. The researchers concluded that connected cars are "a privacy nightmare on wheels" and "the official worst category for products in privacy".[14]

Among the elements analysed in the report, researchers have considered: the amount of personal data collected (which turned out to be much more than necessary); the sharing of the data (whereby 84% of the car brands sold the data to third parties or shared information with government agencies); the control by the driver about the data (92% of the car brands practically gave the driver no possibility of control).

Right after the publication of this report, consumer concerns started becoming an area of increasing interest worldwide. In Australia, a consumer made headlines when he sought a refund of the deposit paid for his Toyota Hilux model, after discovering how his data was related to the connected services of the car. In particular—and this element is common to all experiences in this matter so far, independently of the country and the legal system where Toyota sold its cars –, he noticed that Toyota (as well as the other companies) collected data such as the vehicle location, the driving behaviour, the recording of voices and images in the car and many others by default, unless the consumer decides to opt out. If a person tried to opt out, though, Toyota was sending a warning that this choice would have disabled many features—including Bluetooth and the speaker functionality—that were probably one of the reasons consumers bought the car in the first place. In this case, Toyota not only refused to give back the refund to the consumer, but also initially told the consumer that de-activating the connected services would put at risk even his insurance.[15] It should be incidentally noted that, also thanks to the data collected, Toyota registered in 2024 the total sum of 32 billion of dollars and in 2025 the trend stays positive in terms of connected cars sold.[16]

In terms of legal background, it should be noted that the main piece of privacy regulation in Australia is the Privacy Act of 1988, which is based on a 'notice and consent' model where broad consent is generally considered lawful. In fact, the consent is often given on vague terms and implied in the contract. To make an example, companies such as Toyota can sell and re-sell data to brokers or insurers as long as this possibility is just mentioned in the privacy policy.[17] Moreover, also in the case of an 'opt-in' function, such as *Drive Pulse* (a Toyota function which uses sensor

[13] The report investigated twenty-five car brands, among which Renault, Dacia, tesla, Toyota, Nissan, BMW, Jeep, FIAT, Subaru, and Chrysler.

[14] The report is available at https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[15] About the case, see the reports of the Australian organization CHOICE, that backed up the consumer who first dealt with Toyota, at https://www.choice.com.au/toyotaprivacyinvestigation. See also Kemp (2024).

[16] See https://roadgenius.com/cars/statistics/sales-by-manufacturer/.

[17] Kemp (2024).

data from each trip with a score from 0 to 100, and that intuitively could prejudice the consumer), there is transparency neither about if and when this information will eventually be deleted, nor about whom it could be disclosed to.[18]

As previously mentioned, the case raised concerns and prompted an intense debate around the necessity to reconsider and reform the privacy policies in force in the whole country.[19] The debate forced the Office of the Australian Information Commissioner (OAIC) to ask for a reform of data protection law and to introduce some relevant amendments. Under the Privacy and Other Legislation Amendment Act 2024, adopted in December 2024, individuals have the possibility to sue companies for serious privacy intrusion or misuse of data, and, starting from 2026, companies must disclose in their privacy policies when personal data is used in automated decisions that significantly affect individuals, such as in algorithms or AI systems.[20]

Interestingly, in the U.S., the Attorney General of the state of Texas brought in 2024 an action against General Motors under the allegation of "unlawful collection and sale of over 1.5 million Texans' private driving data to insurance companies without their knowledge or consent".[21] The Attorney claimed that the company literally deceived the customers forcing them to enrol in a program called "OnStar Smart Driver" as if it was an integral part of the vehicle's process of functioning. Moreover, General Motors supposedly also told customers that, failing to enrol, would have caused serious issues in the safety features of the car.

The claim was the object of an investigation promoted also by the Federal Trade Commission (FTC) that concluded General Motors not only did fail to provide consumers with informed consent related to the 'OnStar Smart Driver' app, but also sold the gathered data to some collecting agencies, such as Verisk and LexisNexis, including hundreds of thousands of location data points.[22] As reported by the FTC, this was an "extremely invasive"[23] action. For example, the investigations found that for one consumer GM was able to track all the visits made to a hospital campus during a month, as well as to expose the usual routine of another customer from the usual residence to work, including the precise times and dates of every trip.[24] Both

[18] It is no coincidence that this option is no longer available from April 2025. See the official statements by Toyota on the official website at https://support.toyota.com/s/article/What-is-Drive-Pulse-s-10726?language=en_US.

[19] In this respect, see the study conducted by Katharine Kemp of the UNSW Sidney who analysed all the privacy policies in Australia related to connected cars in 2024, and concluded that a privacy reform was absolutely necessary in order to protect all kinds of information—classified as 'vehicle information'—that, according to Kemp, are instead 'personal information'. Kemp (2024).

[20] Privacy and Other Legislation Amendment Act 2024 (Australia).

[21] Hill (2024). Hill is one of the most prominent investigative reporters for the NYTimes who was the first to uncover the dangers related to the company Clearview, that was the leader in the market of facial recognition. She was also the one to uncover the practice behind the app OnStar Smart Driver.

[22] FTC (2025).

[23] FTC (2025), no 36.

[24] FTC (2025), no 37.

the state of Texas and the FTC underlined how the car company betrayed consumers design the services as extracting data by default.

We could continue describing all the failures contained in the Mozilla's report, showing how incredibly pervasive these companies could be to get to the point to collect data related to the sexual activity of the occupants of the car (Nissan) or to their sexual orientation (such as Kia, which openly states it on its official website when discussing the nature of the information that could be shared by the company with third parties).[25] Any statement made by these companies' top management assuring that this information is never used, becomes irrelevant. What is important here is that this type of data is collected in the first place.

What about Europe? Following the Mozilla's report, concerns about cars' connected services spread across European countries. What has to be noted is that the same report underlines that only two brands—Dacia and Renault—were to be considered less worse and more 'privacy oriented' than the others.[26] In our opinion, it is no coincidence that both companies operate and are available only in Europe and, therefore, are subject to the application of the General Data Protection Regulation (GDPR)[27] and to the EU legislation on privacy and data protection more in general.

The next section looks at the relevant European legal framework in order to map the state of the art in relation to connected services and, in particular, to assess how a case like the Toyota one could occur in Europe.

4 The EU Paves the Way

As we have seen, connected car services inherently raise the problem of the increasing process of personal data—including real-time location, driving behaviour, and in-vehicle communications. In the EU, the legal and ethical implications of such processing have become central to discussions about consumer rights, privacy, and digital trust. The main source to look at in this field is undoubtedly the General Data Protection Regulation (GDPR), together with the European Data Protection Board (EDPB)'s guidelines on connected vehicles and responsible innovation. Of course, there is also a role to play for the AI Act; yet we chose to focus this paper on data protection law, because this is more relevant to the topic here discussed, and because of our interest in privacy. Nevertheless, we cannot but mention that the AI Act is inspired by the principle of 'promotion and protection' that attempts to combine technology and fundamental rights.

---

[25] See the official web site https://www.kia.com/us/en/privacy, about the information the company can collect.

[26] The report is available at https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Although a deep analysis of the GDPR is out of the scope of this paper, it is worth recalling that the European regulation adopts a broad definition of personal data under article 4(1). The definition includes any information relating to an identifiable person, which clearly encompasses location data, vehicle usage patterns, and biometric identifiers such as voice or facial recognition.[28] Article 5 of the GDPR sets out the core principles on data protection among which lawfulness, fairness and transparency, data minimization and accountability are certainly significant for our topic.

While the difficulty of applying article 6(1) of the GDPR on explicit consent is recognized in the ambit of automated data flows in vehicles,[29] consent anyway must meet the strict requirements set forth by article 7 GDPR and must be revocable at any time. The aim of the EDPB Guidelines first published in 2020 and finally adopted in 2021 on the specific theme of connected cars was precisely to clarify the application of the GDPR to the processing of personal data in connected vehicles and mobility-related services, offering practical interpretations and compliance strategies for manufacturers, service providers, and other data controllers in the automotive sector.[30]

The EDPB 2021 Guidelines emphasize that modern vehicles process increasing amounts of personal and sometimes sensitive data, including geolocation, driver behaviour, biometric identifiers, vehicle diagnostics, tied to an identifiable driver**.** Even if some of this data is technical in nature, it becomes personal data when it can be linked to an individual—even indirectly. As the Guidelines state, "[m]ost data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals".[31] The Guidelines reinforce the concepts of privacy by design and by default,[32] stating that manufacturers and service providers must integrate data protection considerations from the outset of the design process; they should therefore prioritize whenever possible processing data locally within the vehicle rather than transmit data to external servers, minimize data flows, offer consent per feature rather than bundled, and so on and so forth.

In addition, data should be collected and stored only as long as necessary, and at the lowest possible level of granularity. Finally, privacy settings must be easily accessible, modifiable, and understandable via the vehicle's human–machine interface (HMI) or companion app.

Notably, the final version of the Guidelines adopted in 2021 stress user controls and privacy setting much more than the previous draft of 2020, and pays substantial

[28] Under article 4, no. 1, GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[29] See, in this respect, Leiser (2024).

[30] EDPB (2021).

[31] EDPB (2021), para 62.

[32] There is a rich literature on this distinction. See for all Ježová (2020), Hustinx (2010), van Dijk, Tanas, Rommetveit, Raab (2018).

attention to optional behavioural contracts like usage-based insurance, for which it requires that an equivalent non usage-based insurance contractis always offered.[33]

A further important point is made with regard to the transmission of data to third parties. As provided for in the guidelines, "only the data controller and the data subject have access to the data generated by a connected vehicle".[34] Nevertheless, "the data controller may transmit personal data to a commercial partner (recipient), to the extent that such transmission lawfully relies on one of the legal bases stated in art. 6 GDPR".[35] The EDPB further recommends that the data subject's consent be obtained before the data are transmitted and not with a pre-ticked box.[36]

Following the extremely rapid and disrupting developments of AI, at the request of the Irish Data Protection Commission (DPC), on December 2024 the EDPB issued under article 64(2) GDPR its Opinion no 28 (hereinafter 'Opinion') to address key uncertainties in relation to some questions connected with the use of AI models.[37] The questions included when and how an AI model can be considered as 'anonymous', how controllers can demonstrate the appropriateness of 'legitimate interest' as a legal basis for data treatment in the development and deployment phases, and what consequences the unlawful processing of personal data in the development phase of an AI model has on the subsequent processing or operation of the AI model.

In the Opinion, the EDPB revisits the classic GDPR three-step assessment for legitimate interest under article 6(1), letter (f), of the GDPR, and applies it to AI use, underlining that data treatment must always be lawful, have a specific interest, must be a necessity and must be balancing.

The Opinion is a landmark because it bridges the GDPR with AI practices. For data protection Supervisory Authorities (SAs) the Opinion offers a series of different instruments to challenge vague privacy claims, enforce model deletion, and require retraining. SAs now have stronger tools to advance technical claims about data safety, identity extraction, and anonymization, and are clearly allowed to intervene at any stage of the AI cycle phase—including its training, deployment, and even after third-party handovers.

Although at present no SAs have so far applied the sanctions provided for in the Opinion, it is worth to note that, shortly before the Opinion's release, the Italian *Garante per la protezione dei dati personali* (the Independent Authority for Privacy and Data Protection) fined OpenAI for the lack of transparency, age verification, lawful basis and legitimate interests of ChatGPT, mirroring in its reasoning the same points highlighted in the EDPB's Opinion.[38]

What the Opinion does is to align AI development with data protection, not changing the law but clarifying how the GDPR applies to fundamental aspects of AI. In this way, the Opinion has a twofold function: it links the AI with the GDPR and at

[33] EDPB (2021), para 77 (Sect. 2.4.1 of the Guidelines) and para 106 (Sect. 3.1.1 of the Guidelines).

[34] EDPB (2021), para 96 (Sect. 2.8 of the Guidelines).

[35] Ibid.

[36] EDPB (2021), para 97 (Sect. 2.8 of the Guidelines).

[37] EDPB (2024).

[38] See https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085432.

the same time reaffirms the crucial role of the GDPR itself, becoming an authentic roadmap to consumers, stakeholders and institutions.

5 A Toyota Case in Italy? Impossible! Still…

Considering the above, it seems useful to review some of the contractual conditions relating to the use of Connected Services offered by Toyota as set out in the Italian version. The contractual conditions are accessible when a user downloads the 'MyToyota' App and registers by creating a personal account, matching personal data with the data that identify the Toyota vehicle.

The privacy section begins with a strong commitment of the company to follow the law and the importance of data protection: "At Toyota, we are committed to complying with the letter and spirit of the Law and engaging in business activities based on transparency and fairness in order to adopt impeccable business behaviour. We believe that in order to build trust with our Customers and provide reliable connected car services, it is critical to protect your Personal Data and be transparent about how it is handled" (authors' translation).

This is followed by a description of the parties involved in data management and the purposes such data is shared for. Among these, the most notable are certainly the use of the connected services and their updates, the improvement of their quality, advertising and marketing campaigns, and IT protection and support.

In relation to the type of data processed, Toyota includes data relating to the account and therefore to identity, such as contact details, device ID, and information about the authorized device (smart phone or tablet). Toyota also collects data that is used to identify the vehicle, including geolocation; this data is functionally conditional on acceptance of the connected services rather than optional.[39] This is ambiguous to say the least: under article 6(1)(a) of the GDPR, consent must be freely given and unbundled. Yet Toyota embeds it within the activation process, which implies that consent may not be truly voluntary or separable from core services.

In relation to the privacy mode, the MyToyota App allows users to disable GPS. While this effectively permits opting out post hoc, it also highlights that: geolocation is on by default once connected services are enabled; disabling it limits access to key functionalities like remote unlock or SOS, which users may effectively need and may be the reason why they chose the car in the first place. This choice too seems to be at odds with the GDPR, which requires opt-out to be as easy as opt-in.[40] The need to actively seek out privacy mode suggests the default is 'tracking-on'—a questionable design from a data protection standpoint. Under the perspective of 'design thinking', the person who may be the user of a product or a service or the recipient of a decision

[39] "If you activate the Connected Services […] your Personal Data will be processed […] In particular position of the vehicle, driving conditions (e.g. accelerations, braking)" (authors' translation).

[40] EDPB (2020), recital 42.

should be at the centre of the methodology for developing products, services, and processes. Scholars from different disciplines have shown that 'design thinking' can be usefully applied to many diverse areas of interests, including in the legal context and in particular in designing user-centred privacy policies and practices.[41]

In relation to the 'Recipients of Data' policy, Toyota contractual conditions further add that personal data can be shared with Toyota Motor Europe, Toyota Connected Europe, KINTO Italia, dealers, service providers, and third parties for marketing and profiling.[42] In theory, data is shared only when necessary or with explicit consent. Yet, these subscriptions, despite being optional, are practically tied to the Connected Services. This makes them de facto mandatory and arguably in breach of the GDPR, which demands transparency in data collection and explicit, granular consent for sharing data with third parties.[43]

Finally, the major data breach that exposed geolocation data of 2.15 million Toyota vehicles for over 9 years raises questions about compliance integrity, given the scale and duration of the leak. As is well-known, article 32 of the GDPR requires appropriate technical security, and articles 33 and 34 require data controllers and data processors to timely notify data protection authorities of data leaks.

Overall, while an 'Australian style' Toyota case seems highly improbable in Italy, due to the applicability of the GDPR, we cannot help but notice that the structure and the design of consent flows by the Italian branch of Toyota—bundled services, default-on tracking, and functional lockout—contribute to create a framework where consumers' consent cannot be meaningfully refused without losing essential services, where third-party data sharing remains opaque, and where security leaks demonstrate the persistence of technical vulnerabilities that seriously affect user privacy. In this perspective, Toyota's current terms and conditions in Italy are likely to fall short of genuine privacy compliance, especially inasmuch as geolocation, telematics, and third-party sharing are functionally inseparable from the provision of connected services.

6 The Societal Structure Model for Privacy

What we have seen so far shows that current privacy regulation puts a lot of responsibility on individual persons: the GDPR, which is considered one of the most advanced models in privacy regulation in the world,[44] still heavily relies on consent and on data

[41] See, e.g., Hendry and Friedman (2021) on the value sensitive design; Introna, Nissenbaum (2000) for the responsible design; for privacy design related issues, see Bygrave (2021), Jasmontaite (2018), Hagan (2017), Cavoukian (2011).

[42] See https://www.toyota.it/e-privacy/destinatari-dei-dati.

[43] See articles 13–14 of the GDPR.

[44] For Solove and Harzgov (2024, 1023), the European privacy regulation is the "crown jewel of data privacy laws".

subjects' rights.[45] The idea behind this choice is to give individuals control over their data. We fully agree that empowerment is an important instrument of democracy and a means of protecting fundamental rights. However, the rise of AI has made it increasingly evident how difficult it is to avoid various levels of nudging techniques that effectively blur the line between influencing and destroying individuals' autonomy in their choices. Examples are numerous and ubiquitous. Consider, for instance, the so-called 'dark patterns' used in video games to essentially 'force' users to purchase additional options through deceptive practices.[46]

The so-called 'Individual Control' model of privacy was born in the 1970s in the United States and rapidly spread through the very well-known mechanism of the 'notice and choice approach', under which companies declared their privacy policies and individuals were free to opt out in case of disagreement. Yet, people more often than not do not read privacy notices, so that the mechanism of notice and choice is completely useless.[47]

In Europe the framework is slightly different since the GDPR requires that consent must be express and affirmative (the so-called opt-in), and provides users with additional rights such as, for example, the right to delete data and the right to be subject to automated decisions.[48] This is certainly a far superior level of protection than the one existing in the US, but still depends very much on the ability of the individual and, as the DiVE project has largely demonstrated through these years, people's vulnerabilities play a major role in the decision process in the digital dimension.

This is why we argue that another way to understand privacy could be more appropriate: the so-called 'Societal Structure' model. This is not a new approach and in fact many academic commentators promoted this approach for a long time.[49] Already in 1987, Simitis was suggesting that "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone".[50] The 'Societal Structure' model of privacy conceptualizes privacy not merely as an individual right or personal preference, but as a relational and institutional construct embedded within broader social, legal, and technological systems. As Reidenberg put it, "society as a whole has an important stake in the contours of the protection of personal information".[51] Schwartz, Gandy, Cohen, Reidenberg, Simitis, and Regan have advocated that privacy must be seen as a societal value, not as merely an individual interest.[52] Other scholars joined and enriched this approach emphasizing how

[45] Gillis and Simons (2019).

[46] The leading case in this matter is Fortnite, a popular video game that went under scrutiny by the Federal Trade Commission for deceptive practices (see https://www.ftc.gov/enforcement/refunds/fortnite-refunds). But dark patterns are practically used everywhere. See Leiser (2025).

[47] See articles 17 and 22 GDPR.

[48] Solove (2024). Richards and Hartzog (2019) detail three 'pathologies of consent', which describe defects consent suffers: unwitting consent, coerced consent, and incapacitated consent.

[49] Reidenberg (2002), Allen (2000), Schwartz (1999), Regan (1995), Simitis (1987).

[50] Simitis (1987, 709).

[51] Reidenberg (2002, 1892).

[52] Schwartz (1999), Gandy (2021), Cohen (2000), Reidenberg (2002), Simitis (1987), Regan (1995).

privacy norms and protections are shaped by structural conditions such as power asymmetries, economic incentives, and regulatory environments.

These scholars recognized that individuals often operate within contexts where meaningful consent is constrained by dependencies on digital infrastructure, social participation, or economic necessity. From this perspective, privacy violations are the result not simply of inadequate personal choices, but of systemic design features—such as default settings, platform architectures, and governance regimes—that limit agency and reinforce surveillance logics. Thus, the societal structure model calls for a shift in focus from individual compliance to collective safeguards and institutional accountability, positioning privacy as a public good whose protection requires structural interventions rather than mere formalistic adherence to consent-based mechanisms. From this perspective, the AI Act appears to be more aligned with the societal model, as it prioritises limiting the risks and harms associated with AI. This could set an example for privacy law to follow.

If we look at our Toyota's connected services case, we can see that the societal structure model of privacy provides a more accurate answer and perspective for understanding data practices in contemporary digital ecosystems. Toyota's contractual and technological architecture reveals how structural forces often outweigh genuine user autonomy. The bundling of essential vehicular functions (navigation, remote diagnostics, emergency services) with broad data processing consents—covering geolocation, telematics, and third-party sharing—creates a scenario in which refusal leads to a substantial loss of functionality.

In this context, consent becomes a procedural formality rather than a meaningful exercise of autonomy. The societal structure model aims at reframing this issue: rather than seeing privacy violations as the result of individual failure to manage settings, it exposes the systemic dynamics—such as design defaults, power asymmetries between users and automakers, and the economic incentives to commodify data—that compel disclosure as a condition of access. In this light, Toyota's practices, though arguably aligned with the formal text of the GDPR, fall short of the regulation's normative intent by exploiting structural dependencies and offering users a constrained set of choices.

The Toyota case highlights very well the limits of the consent-centric framework and the need for privacy governance approaches that prioritize structural safeguards, default protections, and collective accountability over individual responsibility alone.

7 In the Name of Dignity

The case of Toyota's Connected Services shows that the mere prospect of regulatory compliance based exclusively on individual consent is insufficient to understand and prevent the breach of data protection and fundamental rights. In this respect, the deeper normative lens of human dignity, as articulated by Stefano Rodotà in his foundational work on law and technology, should be used to develop a methodology for governing the complex relationship between technological innovations and the law.

According to Rodotà, dignity is not a residual or abstract value but a foundational principle that must guide the design and governance of technological systems, particularly in the digital age. He warned that technological innovation—especially when deployed without ethical or institutional restraint—could easily transform individuals into mere objects of data extraction, eroding their autonomy and agency.

In the Toyota case, users are required to surrender geolocation, behavioural, and biometric data as a condition for accessing essential functions of the car, often through opaque interfaces and bundled consent mechanisms that leave little room for meaningful refusal. As we showed, even if formally aligned with the GDPR consent requirements, Toyota's conditions violate the deeper constitutional and ethical principles Rodotà envisioned, namely, the idea that digital architectures should be designed around people rather than the market.

In Rodotà's view, privacy is not simply an individual right, but a social value rooted in dignity, requiring collective and structural protections. This should also be the view of our institutions. Such a model of data governance reflects a technocratic logic that prioritises efficiency and control over personhood by conditioning fundamental digital mobility services on pervasive surveillance. Reclaiming human dignity in such contexts demands a reorientation of legal frameworks: from a logic of permission and compliance to one of limitation and responsibility, where technology serves the individual rather than the other way around.

References

Albertson Fineman M (2009) The vulnerable subject: anchoring equality in the human condition. Yale J Law Fem 20:1–24

Allen AL (2000) Privacy as-data control: conceptual, practical, and moral limits of the paradigm. Connecticut Law Rev 32:861–875

Bygrave LA (2021) Security by design: aspirations and realities in a regulatory context. Oslo Law Rev 8(3):126–177

Calo R (2017) Privacy, vulnerability, and affordance. DePaul Law Rev 66(2):591–604

Cavoukian A (2011) Privacy by design: the 7 foundational principles. Available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Cohen JE (2000) Examined lives: informational privacy and the subject as object. Stanford Law Rev 52:1373–1437

Crootof R, Kaminski ME, Nicholson Price WII (2023) Humans in the loop. Vanderbilt Law Rev 76:429–510

European Commission (Business Innovation Observatory) (2015) Internet of Things. Connected Cars. 190/PP/ENT/CIP/12/C/N03C01. Available at https://ec.europa.eu/docsroom/documents/13394/attachments/2/translations/en/renditions/native.

European Data Protection Board (EDPB) (2024) Opinion No 28 on certain data protection aspects related to the processing of personal data in the context of AI models. Available at https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.

European Data Protection Board (EDPB) (2021) Guidelines on processing personal data in the context of connected vehicles. Available at https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

European Data Protection Board (EDPB) (2020) Guidelines 05/2020 on consent under Regulation 2016/679. Available at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
Federal Trade Commission (2025) Complaint in the matter of general motors LLC, General Motors Holdings LLC, and Onstar LLC, Docket no 242-3052. Available at https://www.ftc.gov/system/files/ftc_gov/pdf/242_3052_-_general_motors_complaint.pdf
Gandy JROD (2021) The panoptic sort: a political economy of personal information, 2nd edn. Oxford University Press, New York
Gillis TB, Simons J (2019) Explanation < Justification: GDPR and the Perils of Privacy. 2 Pennsylvania J Law Innov 2:71–99
Hagan M (2017) Law by design. Available at https://lawbydesign.com
Hendry DG, Friedman B (2021) Value sensitive design as a formative framework. Ethics Inf Technol 23:39–44
Hill K (2024) Your face belongs to us. A tale of AI, a secretive startup, and the end of privacy. Random House Trade Paperbacks, Toronto-Vancouver
Hustinx P (2010) Privacy by design: delivering the promises. Identity Inf Soc 3(2):253–255
Introna LD, Nissenbaum H (2000) Shaping the web: why the politics of search engines matters. Inf Soc 16(3):169–185
Jasmontaite L et al (2018) Data protection by design and by default. Eur Data Protect Law Rev 4(2):168–189
Ježová DJ (2020) Principle of privacy by design and privacy by default. Regional Law Rev 12:127–139
Kemp K (2024) Driving blind: the unexamined privacy risks of connected car. Available at https://papers.ssrn.com/5025836
Leiser MR (2025) Dark patterns, deceptive design, and the law: AI'S hidden influence on our digital experience. Hart, Oxford
Leiser MR (2024) The question of consent in European data protection. In: Costello RÁ, Leiser M (eds) Critical reflections on the EU's data protection regime: GDPR in the machine. Hart, Oxford
Malgieri G, Niklas J (2020) Vulnerable data subjects. Comp Law Secur Rev 37:105415. Available at https://www.sciencedirect.com/science/article/pii/S0267364920300200
Mendola D, Pera A (2022) Vulnerability of refugees: Some reflections on definitions and measurement practices. Int Migr 60(5):108–121
Nussbaum MC (2000) Women and human development. The capabilities approach. Cambridge University Press, Cambridge
Pera A, Rigazio S (2025) Love (?) is in the web: emotional vulnerability and A.I. girlfriend. In: Diurni A, Amodio C (eds) Human Vulnerability in Interaction with AI. Springer, Cham, forthcoming
Pera A, Rigazio S (2024) Let the children play. Smart toys and child vulnerability. In: Crea C, De Franceschi A (eds) The new shapes of digital vulnerability in European private law. Nomos, Baden-Baden, pp 413–438
Regan PM (1995) Legislating privacy: technology, social values, and public policy. University of North Carolina Press, Chapel Hill
Reidenberg JR (2002) Privacy wrongs in search of remedies. Hastings Law J 54:877–898
Richards N, Hartzog W (2019) The pathologies of digital consent. Washington Univ Law Rev 96:1461–1503
Rodotà S (2014) Il diritto di avere diritti. Laterza, Roma-Bari
Schwartz PM (1999) Privacy and democracy in cyberspace. Vand Law Rev 52:1607–1702
Sharma C, Gordon E (2025) Bailing out biometrics. 18 J Tort L 1. Available at https://ssrn.com/abstract=5312386.
Simitis S (1987) Reviewing privacy in an information society. Univ Pennsylvania Law Rev 135:707–746
Solove DJ (2024) Murky consent: an approach to the fictions of consent in privacy law. BU Law Rev 104:593–640

van Dijk N, Tanas A, Rommetveit K, Raab C (2018). Right engineering? The redesign of privacy and personal data protection. Int Rev Law Compar Technol 32(2):230–256
Viljoen S (2021) A relational theory of data governance. Yale Law J 131:573–654
Zuboff S (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. Public Affairs, New York